Society's New Frontier—Cybersecurity, Privacy and Online Expression

Len Kennedy†

The following is a written adaptation of the opening speech for the 2019 Symposium.

To the *Journal*'s editorial board, the presenters, commentators, audience, and most importantly, the sponsors, I hope you find inspiration in the Symposium's presentations.

The articles presented in this issue touch on important aspects of some very difficult problems—problems that grow as they continue to be analyzed, discussed, and debated. Proposed solutions abound, but consensus does not.

Is there even still agreement about what "data" is? Whatever it might be at its core, what is it when combined with other sources of data? What is it when it has been mined and subjected to proprietary algorithms? The developments among experts are mind-numbing—especially to the non-expert. And in the United States (U.S.), governmental policymakers, while intelligent, are likely non-experts. Nevertheless, legislative action is required to ensure greater protection for consumers, certainty for businesses, and security for society.

Even if we bypass the question of privacy rights, and data as such—how we treat the providers of data and privacy services in the antitrust context is a momentous question. We must engage in complex legal enquiries to address the nature, as well as the beneficial or harmful consequences of the presence and uses of market power.

As the articles of this Symposium suggest, ambitious notions of privacy by design, application of blockchain to shareholder voting and governance, and the use of technology to address questions of appropriate speech offer promise in resolving the questions posed by data and privacy rights. We should be open to the possibilities that these discussions provide. But we must be skeptical as well. Indeed, we would be wise to heed the words of former Secretary of State Dean Acheson: "Always remember that the future comes one day at a time."[1]

---

† Len Kennedy is an award-winning lawyer, corporate executive, and former senior government official with vast experience in the regulation, deregulation, and application of antitrust and public policies to businesses undergoing technological change and rapid growth. B.A., 1974, and J.D., 1977, Cornell University. Member of the Washington, D.C. and Maryland Bars.

1. *See, e.g.*, WILLIAM E. SCHMICKLE, THE HISTORIC DISTRICT ACTION GUIDE: FROM DESIGNATION CAMPAIGNS TO KEEPING DISTRICTS VITAL 396 (2018) (quoting Dean Acheson).

This Symposium was convened at a propitious moment during the global conversation on society's role and the need to regulate the Internet, social media, cybersecurity, privacy, and BIG Tech.[2] The urgent question facing us was: What measures must the government and society—domestically and globally—impose on the conduct, power, and threat that these disruptive technological forces pose even as they add ever greater efficiency, services, productivity, and convenience to our lives.

In 1996, Peter Bernstein cataloged the methods and means of controlling risks to produce desirable societal outcomes.[3] He made a very compelling case for the proposition that the benefits of the aforementioned technological forces have outweighed the costs. Namely, risk management, the evolution of insurance, the insights of finance, and the development of securities markets have made it possible for entrepreneurs and businesses to take on risks and offer new and better products profitably. In turn, this fuels employment, education, and satisfies society's needs and wants.

However, Bernstein's study was a historical one, and it was more narrowly focused than the broad questions we face today. Currently, we have the greater challenge of looking ahead and making decisions in light of recent developments, rapidly changing technology, a global economy, inadequate information, and unduly limited insight. Nevertheless, we must look to our past and to our future in order to choose wisely because our data and privacy rights are at stake.

Recently, McKinsey & Company, a top-tier global consultancy agency, concluded that "[c]ompanies need an understanding of their exposure, vulnerabilities, and potential losses to inform resilience strategies."[4] This insight applies equally, if not more, to governments. The world we now live in is populated with cybercriminals, government-initiated or inspired cyber and social media attacks, data theft, and intellectual property theft. These hostile actors exploit known vulnerabilities and continuously search out new ones. Collectively, they give new meaning to Joseph Schumpeter's term "creative destruction."[5] Ironically, Schumpeter coined this term to define the positive outcomes of competition. However, with respect to cyberattacks and cyber threats, there are no positive outcomes unless it is the interception or failure of the attack. It has rightly been said that "[d]riven by economic interdependence, the race to develop transformational technologies, and the ubiquity of cyberspace, national security and

2. "BIG Tech" refers to "the five largest global [digital] companies (by market capitalization) . . . [that is,] Apple, Alphabet (Google), Microsoft, Facebook, and Amazon." *See* JEAN TIROLE, ECONOMICS FOR THE COMMON GOOD 379 (Princeton Univ. Press 2017).

3. *See generally* PETER L. BERNSTEIN, AGAINST THE GODS: THE REMARKABLE STORY OF RISK (1996).

4. *Risk, Resilience, and Rebalancing in Global Value Chains*, MCKINSEY GLOBAL INST. (Aug. 6, 2020), https://www.mckinsey.com/business-functions/operations/our-insights/risk-resilience-and-rebalancing-in-global-value-chains# [https://perma.cc/5B8M-DRWZ].

5. The term refers to the "incessant" process of creation and destruction that inheres in the capitalist system. A process that Schumpeter believed benefits society. *See* JOSEPH A. SCHUMPETER, CAPITALISM, SOCIALISM AND DEMOCRACY xxiii (Harper Perennial Modern Thought ed. 2008).

economics are converging."[6] In other words, the stakes are high indeed and are of national concern. The authors of *Economic Might, National Security, and the Future of American Statecraft* demonstrate that economic security and national security are joined at the hip.[7] The recent report of the Cyberspace Solarium Commission warns that "a broad array of threat actors are exploiting global connectivity to achieve their objectives,"[8] which are antithetical to the interests of the U.S.

While the COVID-19 pandemic, an unprecedented global health crisis, would seem to exist and require a response independent of issues that are at the heart of this Symposium, reality demonstrates that nothing could be further from the truth. In fact, it exacerbates the subjects we cover and address in this Symposium. For example, in May of 2020, the Commission Co-Chairs, Senator Angus King and Representative Mike Gallagher concluded:

> Over the past two decades, the United States has experienced a barrage of cyberattacks that have impacted the national economy, American democracy, and peoples' daily lives. Despite these shots across the nation's bow, the United States has been slow to correct our course and update our institutions to meet the threat. . . . [T]he COVID-19 pandemic serves as another warning shot, challenging the resiliency of the nation in new ways and underscoring the urgency with which the United States must improve its capacity to prevent, withstand, and respond to crises regardless of their cause.[9]

In other words, "[t]he COVID-19 pandemic has highlighted the universal vulnerabilities inherent to globalization . . . ."[10] It has revealed our complete vulnerability to unexpected threats. Therefore, like COVID-19, the emerging threat of forces presented by technological advances have the power to make systems vulnerable even as they are "improved."

I. The New Frontier

Without doubt, we face significant challenges and a "new frontier." This phrase is fraught with history, meaning, and purpose. To understand it, we must discuss the term "new frontier," as it was understood in the 1960s.

On July 15, 1960, then-presidential candidate John F. Kennedy, in his acceptance speech at the Democratic National Convention in Los Angeles, declared: "[W]e stand today on the edge of a New Frontier—the frontier of

6. *See* David H. McCormick, Charles E. Luftig & James M. Cunningham, *Economic Might, National Security, and the Future of American Statecraft*, Tex. Nat'l Security Rev., Summer 2020, at 1, 3.

7. *Id.*

8. Cyberspace Solarium Commission, Final Report 1, 8 (2020), https://www.solarium.gov [https://perma.cc/YG3A-XF92].

9. *See* Cyberspace Solarium Commission, Cybersecurity Lessons from the Pandemic ii (2020), https://www.solarium.gov [https://perma.cc/YG3A-XF92] [hereinafter Cybersecurity Lessons].

10. *See* McCormick, Luftig, & Cunningham, *supra* note 6, at 17.

the 1960s—a frontier of unknown opportunities and perils—a frontier of unfilled hopes and unfilled threats."[11] At that time, we were in the midst of a Cold War and an intense competition over primacy in outer space. We also faced an existential threat with the Cuban Missile Crisis and the implacable forces behind the Iron Curtain. Therefore, recognizing the dangers posed by miscommunications with a nuclear rival in a time of crisis, we established an around-the-clock "hot line" for direct communication between the Moscow Kremlin and the White House.[12]

Hence, the scientific and engineering prowess of the U.S. was dedicated to connecting our country for voice, video, and fax communications. Deploying bandwidth-limited communications pipes was a costly and slow process, and it was even more expensive when it came to long-distance communication. But it was foremost a national security enterprise that enriched civilian communications as well and sparked the growth of the computer industry. In overcoming those major technological, economic, and engineering challenges, we made the world a smaller place.[13]

II. In My Beginning Is My End

The development of modern communication systems was a difficult journey. While the United States benefited from civilian uses of research and scientific advances funded by the Department of Defense, scholars at Cornell University and around the country worked to make the case for a healthy, civilian economy based on infrastructure investment and competition, rather than regulation. These scholars had concluded that regulatory strictures on economic activity were byproducts of the Great Depression and World War II and were therefore, obsolescent, if not obsolete.[14] This was because a host of government regulatory agencies like the Federal Communications Commission (FCC) and the since-closed Civil Aeronautics Board (CAB), had their origins in that era. Since their creation, however, these agencies have had their authorities modified, updated, or eliminated.

Among the scholars spearheading the discussion were two extraordinary Cornell professors—Alfred Kahn in the Economics Department and Don Baker at the Law School. During my time at Cornell, from 1969 to 1977, I had the opportunity to work with both of these professors. For this

11. John F. Kennedy, The New Frontier, Acceptance Speech at the Democratic National Convention 6 (July 15, 1960) [hereinafter The New Frontier] (transcript available at https://www.jfklibrary.org/asset-viewer/archives/JFKSEN/0910/JFKSEN-0910-015 [https://perma.cc/23NL-6S6D]).

12. *See Memorandum of Understanding Between the United States of America and the Union of Soviet Socialist Republics Regarding the Establishment of a Direct Communications Link*, U.S. DEP'T OF STATE (June 20, 1963), https://2009-2017.state.gov/t/isn/4785.htm #treaty [https://perma.cc/7M2N-L77W].

13. *See* JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: TELECOMMUNICATIONS LAW AND POLICY IN THE INTERNET AGE 1–22 (MIT Press 2d ed. 2013) (describing the decades-long advance of concomitant modernization of regulatory policies).

14. *Id.* at 23–82.

reason, the opportunity to participate in this Symposium is especially meaningful for me.

Dean Kahn, as we called him, was an authority on regulation. From 1970 through 1971, he published his magisterial *The Economics of Regulation: Principles and Institutions*. He later served with distinction in the CAB, the New York State Public Service Commission as Chairman, and the White House as an inflation czar.

Professor Baker, on the other hand, made his name through a long career inside the Antitrust Division of the Department of Justice. He prosecuted stock brokerages, as well as members of the banking, power, and communications industries for what he saw as their anti-competitive practices.

Both men were strong believers in the promise of markets delivering unknown opportunities that would meet the needs of consumers.[15] You might even say they were believers in consumer sovereignty. Based on their studies and investigations, they believed that meaningful choice would benefit the consumer and the marketplace.[16] Although their actions were criticized by businesses, consumer groups, and even regulators, they always operated within the constraints of the law and worked within that institutional framework.

During my time as an Economics major and law student, I drank eagerly of the cup they offered. It was a wonderful experience. When established policy or law did not seem to support our positions, we published articles to convince ourselves and persuade doubters. We also drafted and commented on legislation to help solve the problems we saw. As a result, my professional life is inextricably tied to telecommunications and the development of the policies under which the industry now operates. And I have applied what I learned from them when representing clients before government agencies, courts, the Executive Branch, and Congress.

III. Distinct Markets—Grand Bargain

Throughout the 1960s and 1970s, the introduction of newer, more efficient long-haul capacity brought faster transmission speeds and constant requests to operate networks by large businesses and would-be competitors to AT&T—the then-principal long-distance carrier.[17] FCC licensing of MCI Telecommunications Corp., Sprint, and others led to widespread deployment of communications infrastructure and dramatic price reductions for service. In response, the demand for these services grew faster than the economy as a whole and led to the information and communications technologies (ICT) that today are broadband, operate at high speeds and with great capacity, and are able to combine voice, data,

15. *Id.* at 365–66.
16. *Id.* at 127–58.
17. *Id.* at 23–82.

text, audio files, video, and any other form of digitized information.[18]

The FCC and the courts created several policies that endorsed competition over monopoly.[19] The policies sought and achieved de-monopolization of the telecommunications equipment and service industries, and deregulation of most industry facilities and service providers. Market reliance also necessitated non-discriminatory, cost-based access to local carrier networks. These broad principles where eventually adopted by the Telecommunications Act of 1996 (the Act) in arcane, legislative language that interested parties hashed out at the FCC, the appellate courts, and the U.S. Supreme Court.[20] In addition, the Act also granted a right to physical interconnection.[21] In all, these policies effectively increased the value of all networks making it easier to fund network investments and make a return on said investments. Policymakers also stimulated the market by providing large swaths of spectrum for cellular, wireless fidelity (WiFi), and other terrestrial and satellite services.

With access to the powerful, networked communications infrastructure and freely connected devices, the nascent market for commercial Internet, e-commerce, e-mail, search, information services, online services, and social media exploded. This growth was aided by the high saturation of personal computers, cellular phones (especially the smartphone), the widespread consumer acceptance of software, video games, and other useful services that are now ubiquitous, available globally, and inexpensive. The dominant platforms, search behemoths, and Big Data[22] providers ingeniously built their businesses by stitching these pieces together into appealing service offerings.

The opportunities for enriched lives, social connection, and wealth creation proved to be vast. It is no exaggeration to say that today we stand on the edge of a digital global society. Friedrich Hegel might even have called it a "world-historical" event.[23] That is, an event of enormous significance with stunning consequences no one had foreseen, and no one can evade. Our intensely interconnected world of personal, portable, and two-way communication devices and services allows us to communicate with the world, but also lets the world communicate with us—whether it be for good or for ill.

In spite—or perhaps because of—these successes, we have entered the territory of "unknown perils." In 1960, Kennedy coined this term when discussing the U.S. conflict with the Soviet Union. As a World War II vet-

18. *Id.* at 17–22.
19. *Id.* at 23–82.
20. *Id.* at 127–58.
21. *Id.* at 51–58.
22. The term "Big Data refers to the large, diverse sets of information that grow at ever-increasing rates." *See* Troy Segal, *Big Data*, INVESTOPEDIA (July 5, 2019), https://www.investopedia.com/terms/b/big-data.asp [https://perma.cc/5T94-HLT9].
23. According to Daniel Little, Hegel used the term "world-historical" to refer to "events that were in the process of bringing about the final, full stage of human history and freedom." *See* Daniel Little, *Philosophy of History*, STAN. ENCYCLOPEDIA PHIL. (Feb. 18, 2007), https://plato.stanford.edu/entries/history/ [https://perma.cc/7U6B-XDZJ].

eran, Kennedy was highly attuned to the East-West conflict and necessarily shared the view that our rivalry with the Soviet Union was a zero-sum game with life as we knew it hanging in the balance. It is for these reasons, he called out "unknown perils" and "unfilled threats" as potential roadblocks to fully enjoying the opportunities before us.[24] Our present-day "unknown perils" have changed, but their meaning remains the same. For that reason, we cannot turn the page without full consideration of the increasingly apparent and seemingly vast territory of the "unknown perils" that are now imposed upon us.

Today, far too much of what I read about cybersecurity, privacy, social media, and online expression is alarming, dysfunctional, inadequate, and disconcerting. It suggests that users and customers are not being well-served, and are not being treated like valued customers.[25] To me, all of this indicates that the underlying markets must be reformed and, if need be, regulated to redress perceived market failures or excesses.

Unsurprisingly, leaders in Congress, state capitols, the communications industry, public interest groups, as well as academics and ordinary citizens are calling for just this type of reform, asking that policy and regulatory actions be taken in order to ensure the security of our networks and the integrity of our privacy regimes, social media platforms, and online expression.[26] This Symposium is an opportunity to contribute to the serious debates now underway.

IV. The Existential Peril

Just three years ago, the Defense Science Board (the Board) reported:

> The United States gains tremendous economic, social and military advantages from cyberspace. However, our pursuit of these advantages has created extensive dependencies on highly vulnerable information technologies and industrial control systems. As a result, U.S. national security is at an unacceptable and growing risk.[27]

The Board further found that a "constant barrage of cyber intrusions"

---

24. The New Frontier, *supra* note 11, at 6.

25. *See, e.g.*, *How Good ID Forms the Foundation of Beneficial Tech: A Q&A with Omidyar Network Investment Partner CV Madhukar*, CHRON. PHILANTHROPY, https://www.philanthropy.com/paid-article/how-good-id-forms-the-foundati/316 [https://perma.cc/EHN5-BKDD] ("The speed and scale of technological innovation . . . can exacerbate inequalities, pose new risks, and raise serious issues about responsibility, accountability, and values.").

26. *See generally Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google*, *Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, 116th Cong. (2020) [hereinafter *Online Platforms and Market Power*], *available at* https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=3113 [https://perma.cc/7MQM-3DT5].

27. *See Task Force on Cyber Deterrence*, DEF. SCI. BOARD 1, 1 (Feb. 2017), https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf [https://perma.cc/Y9M3-UPNJ].

occur daily in the U.S. and elsewhere.[28] These cyber intrusions range from nation-state cyber espionage to various cyberattacks, including China's alleged intellectual property theft and Russia's alleged interference with the 2016 presidential election—all of which, if true, harm the United States.[29]

Moreover, the Board explained that the United States, so far, has not suffered the "high end" attack that our best-equipped competitors could mount.[30] Nor have we suffered the "more daunting" threats the Board expects we will face in the coming years.[31] But it emphasized that "[a] large-scale cyber attack [sic] on civilian critical infrastructure could cause chaos by disrupting the flow of electricity, money, communications, fuel, and water."[32] While the report identifies the numerous actions we are taking and must take against these intrusions, cumulatively they subject our nation to "death by 1,000 hacks."[33] Furthermore, U.S. critical infrastructure improvements "are not on a pace to reduce risks to acceptable levels within the next decade."[34] And some developments like "[t]he introduction of massive numbers of digital sensors (the so-called Internet of Things), processors, and autonomous devices to today's internet will only exacerbate an already tenuous situation and make defense even more challenging in the coming years."[35] Therefore, "[t]he unfortunate reality is that for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential [competitors] are likely to far exceed the United States' ability to defend and adequately strengthen the resilience of its critical infrastructures."[36]

Last year, Daniel Coats, then-Director of National Intelligence, delivered his Worldwide Threat Assessment on behalf of the U.S. Intelligence Community to Congress.[37] His assessment covered a range of topics that greatly exceed the scope of this Symposium. Nevertheless, it lists the increasing use of cyber capabilities—cyber espionage, cyberattacks, and influence operations—to seek political, economic, and military advantages as a major threat. Director Coats also mentioned the possible interference with the 2020 presidential election as a likely threat. Therefore, according to his report, the U.S. might experience cyber-based efforts to manipulate or disrupt the election system, tamper with voter registration, and obstruct vote tallying.[38]

Federal and state officials are now working closely to monitor these issues. On August 7, 2020, the United States Intelligence Community (IC)

28. *Id.* at 2.
29. *Id.* at 1–4.
30. *Id.* at 2.
31. *Id.*
32. *Id.*
33. *Id.* at 4.
34. *Id.*
35. *Id.*
36. *Id.*
37. *See generally* Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community*, DIRECTOR NAT'L INTELLIGENCE (2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR—-SSCI.pdf [https://perma.cc/T28Q-9EXA].
38. *Id.* at 5–7.

released its unclassified, election threat information update to the American public.[39] In its unclassified report the IC expressed concerns about allegedly ongoing and potential covert activities by China, Russia, and Iran. The IC has also been providing classified, election threat briefings to the presidential campaigns, political committees, and all members of Congress.[40]

Relatedly, Heather Adkins, the Director of Information Security and Privacy at Google, spoke at Harvard's Belfer Center about election security. She emphasized that in a physical space, you have your five senses, and a sixth sense that tells you when you are in danger, and when you should feel fear.[41] But you do not have a sixth sense in the online world.[42] That is, we do not have a digital sense telling us when we are entering a virtual wormhole. Yet, we have a population dependent on all things electronic all the time.

Fortunately, however, our digital sense is starting to evolve. We are developing what some call "digital hygiene," by learning, adapting, and becoming more skeptical while we are in the digital realm. Long ago, we learned not to leave banks' vault doors open. Now, it is time to protect our digital vaults—whether the assets inside are as small as our credit card numbers or as big as our electric grid and our democratic institutions—because the gains we have made in terms of personal convenience may no longer outweigh the threat to personal and public safety.

As International Business Machines' (IBM) Executive Chairwoman Ginni Rometty warned:

> [D]ata is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true—even inevitable—then cyber crime [sic], by definition, is the greatest threat to every profession, every industry, every company in the world.[43]

Chairwoman Rometty is right. But the growing menace of cyber warfare, cyber-crime, and malicious conduct she referenced may extend to our democracy as well.

---

39. Press Release, Director of Nat'l Intelligence, Statement by NCSC Director William Evanina: Election Threat Update for the American Public (Aug. 7, 2020) (available at https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public [https://perma.cc/JB4U-GZ3U]).

40. *Id.*

41. *See* Heather Adkins, Director of Information Security and Privacy at Google, The Digital Threat to Democracy, Address at the Harvard Kennedy School Forum (Sept. 11, 2017) (transcript available at https://www.belfercenter.org/event/digital-threat-democracy#!transcript [https://perma.cc/9RY3-PY6S]).

42. *Id.*

43. Steve Morgan, *IBM's CEO on Hackers: 'Cyber Crime is the Greatest Threat to Every Company in the World'*, FORBES (Nov. 24, 2015, 6:46 AM) (quoting Ginni Rometty, IBM Corp.'s Chairman, President, and CEO), https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#3a0c8d5a73f0 [https://perma.cc/ZX8G-8JJD].

For example, other ways to threaten a democracy—in addition to election tampering—include destroying trust in the democratic institutions, encouraging apathy, and sowing discord and division through the nation. These actions cause civil society seemingly to implode on its own, and they can be easily carried out.

For example, our competitors could use social media platforms like Facebook and Google. This is similar to the information-dissemination practices that were allegedly used in the past by Komitet Gosudarstvennoy Bezopasnosti (KGB) agents. It was allegedly reported that these agents would bribe reporters and plant stories in the mainstream press.[44] Similar content-manipulation could be conducted in the digital realm.

Roger McNamee, an early investor in Facebook, recently published a fascinating book, *Zucked*, about the way Facebook executives dismissed his concerns that bad actors were infiltrating Facebook and manipulating algorithms and news feeds. In his book, McNamee raises serious concerns about Internet platform monopolies jeopardizing the health of our political system. For that reason, McNamee calls for significant regulatory fixes that Congress is considering and may implement in the future.[45]

The Internet of Things is another unguarded gateway.[46] The Internet of Things refers to interconnected household or business objects such as voice-activated digital assistants, baby cameras, home security systems, and smart TVs. These systems often have poor security and numerous vulnerabilities because manufacturers of these devices fail to build sufficient, internal security controls. Fortunately, however, the National Institute of Standards and Technology (NIST) is under a directive to develop technical standards and best practices for product design, software updates, defect reporting, and other techniques to make these systems more secure in the future.[47] More importantly, the Cybersecurity Solarium Commission recommended that Congress address these vulnerabilities by enacting an Internet of Things Security Law.[48]

Consequently, in order to better defend ourselves from malicious cyberattacks, we need an effective deterrent policy against cyberwarfare. Imagine what would happen if our water and sewer systems, which are digitally controlled and connected to the Internet, were taken down by a hostile actor. Or think about what would happen if the same was done to our regional power grids, which are all connected nationwide. Consider how many industries are dependent on gasoline and diesel pumps, which

---

44. See Adam Taylor, *Before 'Fake News,' There was Soviet 'Disinformation'*, WASH. POST (Nov. 26, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/11/26/before-fake-news-there-was-soviet-disinformation/ [https://perma.cc/PGT7-4F6G].

45. *See generally* ROGER MCNAMEE, ZUCKED (2019).

46. *Task Force on Cyber Deterrence*, *supra* note 27, at 4.

47. *Core Cybersecurity Feature Baseline for Securable IoT Devices: Draft NISTIR 8259 Available for Comment*, NIST (July 31, 2019), https://www.nist.gov/news-events/news/2019/07/core-cybersecurity-feature-baseline-securable-iot-devices-draft-nistir-8259 [https://perma.cc/87TM-VQ4D].

48. *See* CYBERSECURITY LESSONS, *supra* note 9, at 2.

are also controlled digitally and dependent on electricity. Hospital generators, for example, depend on diesel fuel. Everything from banks and ATMs to our military installations could be affected by such a cyberattack. Yet we do not have defined consequences for these hostile actions. And even if we did, credible deterrence would depend on the ability to enforce those consequences. Therefore, we must not only define what the consequences will be, but also ensure that we have the ability to identify perpetrators and implement said consequences if need be.

Thankfully, the Defense Advanced Research Projects Agency (DARPA) is performing a large-scale study on how best to prevent and deter cyberattacks on our power grid.[49] But we cannot leave it solely to the experts. There is much that we can do at an individual level to ignite change.

First, as empowered citizens, we should demand transparency in social media. For example, by asking that the same disclosure rules for political advertising that govern television, radio, and newspapers apply to social media platforms. Second, we should insist on stronger security systems in the Internet of Things. Lastly, we must undertake public and private activities in order to: (1) lessen the vulnerabilities in digital and social media; (2) reasonably regulate and/or incentivize powerful platforms like Google, Facebook, Amazon, Apple, and others; (3) protect elections at both the state and federal levels; and (4) create credible deterrence policies.

Fortunately, on July 29, 2020, the United States Congress convened a hearing to consider and address the steps needed to regulate or restructure BIG Tech, in order to ensure greater competition, freedom of choice, and more competitive rules.[50] This will prevent a small number of very powerful firms from controlling the industry and hindering innovation and service improvements. The goals of regulation should include optimizing privacy and data protection, improving business practices and antitrust remedies, and ensuring the security of devices and networks. We can no longer rely solely upon the free market approach adopted over twenty-five years ago to address the modern technologies that monitor how we live and interact, and how service providers collect, distribute, and commercialize our words, thoughts, images, actions, and sounds.

---

49. *See* Walter Weiss, *Rapid Attack Detection, Isolation and Characterization Systems (RADICS)*, DARPA, https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems [https://perma.cc/EV2F-5URP].

50. *See Online Platforms and Market Power*, *supra* note 26.