EMERGING
THREATS

THE FAILURE OF INTERNET FREEDOM

BY JACK GOLDSMITH

KNIGHT
FIRST AMENDMENT
INSTITUTE
at Columbia University

EMERGING
THREATS

ABOUT EMERGING THREATS

The Knight First Amendment Institute's *Emerging Threats* series invites leading thinkers to identify and grapple with newly arising or intensifying structural threats to the system of free expression. These threats may be caused by changes in the forms and applications of technology, in the means and economics of communication, in the norms and practices of politics, or in legal doctrine. The papers in the series explore ways to address these threats and preserve the foundations of democracy essential to healthy open societies, including the United States.

The *Emerging Threats* series is edited by David Pozen, professor at Columbia Law School and inaugural visiting scholar at the Knight Institute.

ABOUT THE KNIGHT INSTITUTE

The Knight First Amendment Institute is a non-partisan, not-for-profit organization established by Columbia University and the John S. and James L. Knight Foundation to defend the freedoms of speech and press in the digital age through strategic litigation, research, and public education. For more information, please visit www.knightcolumbia.org.

ABOUT THE AUTHOR

Jack Goldsmith is the Henry L. Shattuck Professor at Harvard Law School, a Senior Fellow at the Hoover Institution, and co-founder of Lawfare. He teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws. His books include *Power and Constraint: The Accountable Presidency After 9/11* (2012); *The Terror Presidency: Law and Judgment Inside the Bush Administration* (2007); and (with Tim Wu) *Who Controls The Internet? Illusions of a Borderless World* (2006). Before joining Harvard, Goldsmith served as Assistant Attorney General, Office of Legal Counsel from 2003-2004, and Special Counsel to the Department of Defense from 2002-2003. He was a professor at the University of Chicago Law School from 1997-2002, and at the University of Virginia School of Law from 1994-1997. Goldsmith clerked for Supreme Court Justice Anthony M. Kennedy from 1990-1991, for Court of Appeals Judge J. Harvie Wilkinson from 1989-1990, and for Judge George Aldrich on the Iran-U.S. Claims Tribunal from 1991-1993.

TABLE OF CONTENTS

THE FAILURE OF INTERNET FREEDOM

Jack Goldsmith

From the second term of the Clinton administration to the end of the Obama administration, the U.S. government pursued an "internet freedom" agenda abroad. The phrase "internet freedom" signaled something grand and important, but its meaning has always been hard to pin down. For purposes of this paper, I will use the phrase to mean two related principles initially articulated by the Clinton administration during its stewardship of the global internet in the late 1990s.

The first principle is that "governments must adopt a non-regulatory, market-oriented approach to electronic commerce," as President Clinton and Vice President Gore put it in 1997.[1] Their administration opposed government taxes, customs duties and other trade barriers, telecommunications constraints, advertisement limitations, and most other forms of regulation for internet firms, communications, or transactions. The premise of this commercial non-regulation principle, as I'll call it, was that "the Internet is a medium that has tremendous potential for promoting individual freedom and individual empowerment" and "[t]herefore, where possible, the individual should be left in control of the way in which he or she uses this medium."[2] In other words, markets, individual choice, and competition should presumptively guide the development of the internet. When formal governance is needed, it should be supplied by "private, nonprofit, stakeholder-based" institutions not tied to nations or geography.[3] The Clinton administration acknowledged the need for traditional government regulation in narrow circumstances—most notably, and self-servingly, to protect intellectual property—but otherwise strongly disfavored it.[4]

The second principle of internet freedom, which I'll call the *anti-censorship principle*, argued for American-style freedom of speech and expression on the global internet. This principle originated as a component of the effort to promote electronic commerce. Over time, however, it developed into an independent consideration that sought to influence foreign political structures. The Clinton administration devoted less policy attention to the

* For comments on the ideas in this paper, I thank Yochai Benkler, Rishabh Bhandari, Adam Klein, David Pozen, Stuart Russell, Tim Wu, Jonathan Zittrain, workshop participants at the Belfer Center's Cyber Security Project and at Harvard's Program on Constitutional Government, and commentators at a "Talks at Google" presentation. I also thank those who commented on the version of this paper that I presented as the Brainerd Currie memorial lecture at Duke Law School on March 6, 2018. I thank Devyani Aggarwal, Andrei Gribakov, and Robert Nelson for excellent research and related assistance.

[1] President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce* (1997), https://clinton-whitehouse4.archives.gov/WH/New/Commerce/read.html; *see also* Ira C. Magaziner, Progress & Freedom Found., *Creating a Framework for Global Electronic Commerce* (July 1999), http://www.pff.org/issues-pubs/futureinsights/fi6.1globaleconomiccommerce.html (arguing "against a traditional regulatory role for government").

[2] Magaziner, *supra* note 1.

[3] *Id*. The most notable stakeholder-based experiment was the internet's naming and numbering system. *See* Management of Internet Names and Addresses, 63 Fed. Reg. 31741 (June 10, 1998).

[4] On privacy, for example, the Clinton administration "favored the formation of industry or private sector self-regulation" but acknowledged that "there may be certain cases where, as a backup, government action will be needed" in "very precise ways to address the voids left by self-regulation." Magaziner, *supra* note 1.

anti-censorship principle than to the commercial non-regulation principle because it believed that "[c]ensorship and content control are not only undesirable, but effectively impossible," as the administration's internet czar Ira Magaziner put it.[5] China's effort "to crack down on the Internet," Bill Clinton famously quipped in 2000, was "like trying to nail Jell-O to the wall."[6]

The George W. Bush administration embraced both internet freedom principles, and it took novel institutional steps to push the anti-censorship principle. In 2006, the State Department established the Global Internet Freedom Task Force (GIFT). The main aims of GIFT were to "[m]aximize freedom of expression and the free flow of information and ideas," to "[m]inimize the success of repressive regimes in censoring and silencing legitimate debate," and to "[p]romote access to information and ideas over the Internet."[7] GIFT provided support for "unfiltered information to people living under conditions of censorship," and it established "a $500,000 grant program for innovative proposals and cutting-edge approaches to combat Internet censorship in countries seeking to restrict basic human rights, including freedom of expression."[8] In this way, the Bush administration got the U.S. government openly in the business of paying for and promoting "freedom technologies" to help break authoritarian censorship and loosen authoritarian rule across the globe.

The Obama administration continued to advocate for the commercial non-regulation principle and further expanded the United States' commitment to the anti-censorship principle.[9] The landmark statement of its approach, and the most elaborate and mature expression of the American conception of internet freedom, came in Secretary of State Hillary Clinton's much-lauded January 2010 speech on the topic.[10] Invoking American traditions from the First Amendment to the Four Freedoms, Clinton pledged American support for liberty of speech, thought, and religion on the internet and for the right to privacy and connectivity to ensure these liberties for all. Clinton's successor to GIFT, the State Department's NetFreedom Task Force, oversaw "U.S. efforts in more than 40 countries to help individuals circumvent politically motivated censorship by developing new tools and providing the training needed to safely access the Internet."[11] Other federally funded bodies served similar goals.[12]

---

[5] *Id.*

[6] *Clinton's Words on China: Trade Is the Smart Thing*, N.Y. Times (Mar. 9, 2000), https://www.nytimes.com/2000/03/09/world/clinton-s-words-on-china-trade-is-the-smart-thing.html.

[7] U.S. Dep't of State, *Global Internet Freedom Task Force* (information released online from Jan. 20, 2001 to Jan. 20, 2009), https://2001-2009.state.gov/g/drl/lbr/c26696.htm. GIFT added an assessment of internet freedom to the State Department's annual human rights report and established the institutional machinery to monitor and protest "serious incidents of Internet repression." U.S. Dep't of State, *Global Internet Freedom Task Force (GIFT) Strategy: A Blueprint for Action* (Dec. 28, 2006) [hereinafter GIFT Blueprint], https://2001-2009.state.gov/g/drl/rls/78340.htm.

[8] GIFT Blueprint, *supra* note 7.

[9] *See generally* Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, ch. 12 (2012).

[10] Secretary of State Hillary Rodham Clinton, *Remarks on Internet Freedom* (Jan. 21, 2010), https://foreignpolicy.com/2010/01/21/internet-freedom.

[11] Cong. Research Serv., R41837, *Promoting Global Internet Freedom: Government and Industry Initiatives* 2 (2016).

[12] *See, e.g.*, Open Technology Fund, *About the Program*, https://www.opentech.fund/about/program (last visited May 22, 2018) (describing how a component of Radio Free Asia supports "research, development, and implementation programs focused on increasing … [a]ccess to the internet, including tools to circumvent website blocks, connection blackouts, and widespread censorship").

The Obama administration spent at least $105 million on these programs, which included investment in encryption and filter-circumvention products and support to fight network censorship abroad.[13]

Across administrations, the U.S. internet freedom project has pursued numerous overlapping aims. It has sought to build a stable and robust global commercial internet. It has sought to enhance global wealth—especially the wealth of the U.S. firms that have dominated the computer and internet technology industries. It has sought to export to other countries U.S. notions of free expression and free trade. And it has sought to impact politics abroad by spreading democracy with the ambitious hope of ending authoritarianism. "The Internet," Magaziner proclaimed, is "a force for the promotion of democracy, because dictatorship depends upon the control of the flow of information. The Internet makes this control much more difficult in the short run and impossible in the long run."[14] The Bush administration and especially the Obama administration engaged in high-profile and expensive diplomatic initiatives to use and shape the internet to spread democracy and human rights.

The U.S. internet freedom project deserves significant credit for the remarkable growth of the global internet, and especially global commerce, in the last two decades. But on every other dimension, the project is failing, and many of its elements lie in tatters. In response to perceived American provocations, other nations have rejected the attempted export of American values and are increasingly effective at imposing their own values on the internet. These nations have become adept at clamping down on unwelcome speech and at hindering the free flow of data across and within their borders. Authoritarian countries, in particular, are defeating unwanted internet activities within their borders and are using the internet to their advantage to deepen political control. The optimistic hope that the internet might spread democracy overseas has been further belied by the damage it has done to democracy at home. Digital technologies "are not an unmitigated blessing," Secretary Clinton acknowledged in her 2010 speech.[15] She understated the point. The relatively unregulated internet in the United States is being used for ill to a point that threatens basic American institutions.

I. Hypocrisy

Hillary Clinton's 2010 speech took place against the background of fifteen years of growing global digital conflict.[16] On the surface, this conflict was mostly about control over internet content. The internet was an American invention that, in its very code, seemed to embody the American values of free speech and resistance to regulation. But global connectivity and access initially challenged local political control and sparked resentment and fear among governments in authoritarian and non-authoritarian states alike. These sentiments were exacerbated by the fact that the American technology giants—Amazon, Google, Facebook, Apple, and Microsoft—dominated online life, raking in hundreds of billions of dollars in profits through the relentless growth

[13] *See Review of Resources, Priorities, and Programs in the FY 2017 State Department Budget Request: Hearing Before the Subcomm. on W. Hemisphere, Transnat'l Crime, Civilian Sec., Democracy, Hum. Rts., and Global Women's Issues of the S. Comm. on Foreign Relations*, 114th Cong. (2016) (testimony of Assistant Secretary Tom Malinowski), https://www.foreign.senate.gov/imo/media/doc/042616_Malinowski_Testimony.pdf. The figure may be as high as $145 million. *See* U.S. Dep't of State, *Internet Freedom* (archived June 9, 2017), https://web.archive.org/web/20170609001151/https:/www.state.gov/j/drl/internetfreedom/index.htm.

[14] Magaziner, *supra* note 1.

[15] Clinton, *supra* note 10.

[16] For background, see generally Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (2006).

of their increasingly indispensable digital products. They were also stoked by the United States' control of the naming and numbering system for the internet.[17]

More than any other nation, China fought back against these trends. It developed powerful systems of censorship and control over the internet in order to protect the Communist Party and the nation from what the Party viewed as subversive online forces. And it forced American firms seeking to do business in China to play by its rules or be denied access. Other authoritarian nations took steps in this direction, although none matched China's vigor or commitment.[18]

But it wasn't only authoritarian governments that the U.S. internet freedom project threatened. Europe's prevailing conception of government's relationship to the individual, and the individual's relationship to personal data, differs sharply from the prevailing American conception. Since the 1990s, European regulators have held American technology firms to higher standards of privacy and competition than American regulators have required of them. European regulators have also sought to eliminate from their networks hate speech that is tolerated by the First Amendment but is illegal in Europe.[19]

Below the surface of disputes about content was a different but no less fierce battle about theft of private and proprietary data. Computer systems are inevitably filled with vulnerabilities that can be exploited to gain entry. When a computer is connected to the internet, actors from around the globe have potential access. And the internet's architecture makes anonymity and spoofing (fake emails or webpages disguised to appear genuine) easy, which further facilitates unauthorized entry. The combination of these factors sparked a growing wave of cybertheft in the first decade of the twenty-first century.

The U.S. government participated in this bonanza of digital extraction, although it focused on acquiring military and intelligence secrets rather than commercial theft to benefit U.S. firms.[20] But the United States was also among the most digitally dependent of nations, and a good deal of its military and economic and cultural power was embedded in digital networks. By the time of Hillary Clinton's 2010 speech, the United States worried that it was losing more from cybertheft than it was gaining. American government networks suffered embarrassing intrusions that resulted in the exfiltration of cherished intelligence and military secrets.[21] Just as alarming was the digital theft from abroad of the commercial secrets of American firms. U.S. companies reportedly lost hundreds of billions of dollars of commercial value each year in what National Security Agency (NSA) Director Keith Alexander described

[17] *See id.* at chs. 3, 10. The United States relinquished this control in 2016. *See* ICANN, *Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends* (Oct. 1, 2016), https://www.icann.org/news/announcement-2016-10-01-en.

[18] *See* Goldsmith & Wu, *supra* note 16, at ch. 6.

[19] *Id.* at chs. 1, 10.

[20] *See* Samuel J. Rascoff, *The Norm Against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections*, 83 U. Chi. L. Rev. 249 (2016).

[21] *See, e.g.*, Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. Times (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html; Franz-Stefan Gady, *New Snowden Documents Reveal Chinese Behind F-35 Hack*, Diplomat (Jan. 27, 2015), https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack.

as "the greatest transfer of wealth in history."[22] China was public enemy number one for this great digital heist. But other nation-state adversaries and sophisticated organized crime networks also figured out how to steal information from American computer systems.

One important innovation in Clinton's 2010 speech was to tie the imperative of internet security to the ideal of internet freedom. She did so by drawing on the fourth of President Franklin Roosevelt's Four Freedoms, the freedom from fear. The United States must "work against those who use communication networks as tools of disruption and fear," Clinton said.[23] Nations and individuals that "engage in cyberattacks should face consequences and international condemnation."[24] To further resist the rise of cyberattacks, the United States should "create norms of behavior among states and encourage respect for the global networked commons."[25]

The hypocrisy in the linkage between internet freedom and internet security was apparent even before Clinton finished her speech. Eight paragraphs after complaining about cyberattacks, she boasted that the State Department was "supporting the development of new tools" to fight authoritarian censorship online.[26] These tools—which, as noted above, were supported by tens of millions of dollars in U.S. grants—were designed to help activists advocate for freedom in foreign networks in ways that foreign governments viewed as disrupting those networks and violating their sovereignty.

Authoritarian states had worried since the 1990s about ties between the U.S. government and U.S. technology firms; they feared that the United States would use its internet dominance to foster regime openness and regime change.[27] Their fears grew as U.S. internet technology firms rose to global dominance in the 2000s and as American social media companies like Facebook and Twitter seemed to provide the organizational tools for the protests that shook the Arab world during the Obama administration. In the midst of the demonstrations in Iran following its 2009 presidential election, a State Department official asked Twitter to delay a scheduled maintenance of its network that might "cut off service while Iranians were using Twitter to swap information and inform the outside world about the mushrooming protests around Tehran," as the *New York Times* put it in a story titled *Washington Taps Into a Potent New Force in Diplomacy*.[28] The event confirmed for Iranian officials that "the Internet is an instrument of Western power and that its ultimate end is to foster regime change in Iran," as Evgeny Morozov noted.[29] Iran and other authoritarian governments saw U.S. social media firms in particular as "a 'made in America' digital missile that could undermine authoritarian stability."[30]

That perception intensified after Secretary Clinton delivered a second speech on internet freedom in January 2011, during the early days of the Arab Spring. Clinton emphasized how much Facebook and Twitter had

[22] Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History*," Foreign Pol'y (July 9, 2012), https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history.
[23] Clinton, *supra* note 10.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *See* Alexander Klimburg, *The Darkening Web: The War for Cyberspace* 104–10, 211–12, 327–28 (2017).
[28] Mark Landler & Brian Stelter, *Washington Taps Into a Potent New Force in Diplomacy*, N.Y. Times (June 16, 2009), https://www.nytimes.com/2009/06/17/world/middleeast/17media.html.
[29] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* 10 (2011).
[30] *Id.* at 236.

aided the Arab Spring and touted U.S. financial and technical support "to help people in oppressive Internet environments get around filters [and] stay one step ahead of the censors."[31] That same month, the State Department intervened with U.S. tech companies to help protect protesters in Tunisia who would soon force President Zine El Abidine Ben Ali to step down.[32] As former NSA and Central Intelligence Agency (CIA) director Michael Hayden described these efforts, "The Secretary of State is laundering money through NGOs to populate software throughout the Arab world to prevent the people in the Arab street from being tracked by their government."[33] Authoritarian nations got the message.

The United States also seemed to be militarizing cyberspace in ways that were hard to square with its rhetorical commitment to digital security. Seven months before Clinton's 2010 speech, the Obama administration established U.S. Cyber Command to integrate American cyber operations, including offensive military cyber operations abroad.[34] It was no accident that the administration placed the director of the NSA in charge of Cyber Command. NSA is responsible for breaking into and extracting intelligence from communications and computer systems abroad—activities that are typically prerequisites to the computer network attacks contemplated for Cyber Command. "We have U.S. warriors in cyberspace [who] are deployed overseas and are in direct contact with adversaries overseas," bragged Bob Gourley, a former chief technology officer for the Defense Intelligence Agency, to a reporter a few months after Cyber Command was created.[35] These experts "live in adversary networks," he added.[36]

The astounding degree to which the U.S. government lived in adversary networks would became apparent to the world over the next few years. In November 2010, diplomatic cables pilfered by Chelsea Manning and published by WikiLeaks showed that Clinton herself had sent diplomatic directives about ways to break into the communications channels of diplomats from several nations as well as of the secretary general of the United Nations.[37] This is a standard secret intelligence practice, but it was nonetheless embarrassing for Clinton, who had insisted a few months earlier that "in an internet-connected world, an attack on one nation's networks can be an attack on all."[38]

Then, in June 2012, the *New York Times* reported that President Obama had used an elaborate cyberattack to disrupt the centrifuges in Iran's nuclear enrichment facilities.[39] "Olympic Games," as the operation was called,

---

[31] Secretary of State Hillary Rodham Clinton, *Remarks on Internet Freedom* (Feb. 15, 2011), https://www.eff.org/files/filenode/clinton_internet_rights_wrongs_20110215.pdf.

[32] *See* Joseph Marks, *Hillary Clinton: 'Internet Freedom' Activist?*, Politico (Aug. 10, 2015), https://www.politico.com/story/2015/08/hillary-clinton-2016-internet-freedom-121229.

[33] Shane Harris & John Hudson, *Not Even the NSA Can Crack the State Dept's Favorite Anonymous Network*, Foreign Pol'y (Oct. 4, 2013), https://foreignpolicy.com/2013/10/04/not-even-the-nsa-can-crack-the-state-depts-favorite-anonymous-network.

[34] *See* Memorandum from Secretary of Defense, Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (June 23, 2009), https://fas.org/irp/doddir/dod/secdef-cyber.pdf.

[35] Shane Harris, *The Cyberwar Plan, Not Just a Defensive Game*, Nextgov (Nov. 13, 2009), https://www.nextgov.com/cybersecurity/2009/11/the-cyberwar-plan-not-just-a-defensive-game/45303.

[36] *Id.*

[37] *See* Robert Booth & Julian Borger, *US Diplomats Spied on UN Leadership*, Guardian (Nov. 28, 2010), https://www.theguardian.com/world/2010/nov/28/us-embassy-cables-spying-un.

[38] Clinton, *supra* note 10.

[39] David E. Sanger. *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

marked a new era in the militarization of cyberspace, according to Hayden, because it was "the first attack of a major nature in which a cyberattack was used to effect physical destruction" rather than simply to steal data or disrupt a computer's normal operation.[40] "Somebody crossed the Rubicon," he stated, comparing the attack on Iran to August 1945, when the world first witnessed the destructive power of nuclear weapons.[41] Olympic Games, on top of Cyber Command, accelerated the global arms race for cyber weapons and cyber forces, with ominous implications for internet freedom.

And finally, in the spring of 2013, Edward Snowden stole many thousands of documents from the NSA and gave them to a group of journalists to publish. The documents revealed that the NSA had penetrated every conceivable form of computer and communications system around the globe, sweeping up unfathomable masses of electronic intelligence about foreign governments and foreign citizens.[42] They also showed that it had set up a system to collect huge quantities of intelligence information, not just by breaking into foreign networks but also by (among other means) demanding information from Google, Yahoo!, Facebook, and other American firms that themselves collected data from abroad, especially communications of individuals.[43] In these and other ways, the NSA seemed to be succeeding in its stated aim of (as one of the leaked documents put it) achieving "global network dominance."[44]

"It would be hard to overstate the extent to which Edward Snowden's disclosures about US mass surveillance techniques in the post-9/11 period have shaken up geopolitical dynamics on Internet freedom, security and governance," wrote Eileen Donahoe of Human Rights Watch two years after the leaks.[45] The Snowden disclosures, on top of everything else, gravely damaged the internet freedom project.

They made it seem like the United States' "hands-off" approach to the internet was, as many nations had feared, a mask for U.S. government manipulation and control. They thus exacerbated the resentment that had been building against the United States due to U.S. firms' dominance of the internet economy and the U.S. government's control over the internet's naming and numbering system. The disclosures also showed that the NSA was heavily involved, on a global scale, in the very forms of surreptitious network surveillance that the U.S. government decried when done by authoritarian nations, albeit for different ends. They indicated that the NSA was secretly trying to undermine the very encryption tools that the State Department and other U.S. agencies were promoting to fight oppression abroad.[46] And the disclosures revealed that the United States was acting directly contrary to the cybersecurity imperative that Clinton had linked to the internet freedom agenda in 2010.

---

[40] *Id.*

[41] *Id.*

[42] *See generally Snowden Revelations*, Lawfare, https://lawfareblog.com/snowden-revelations (last visited May 22, 2018) (compiling revelations by Snowden).

[43] These revelations concerned collection primarily under Section 702 of the Foreign Intelligence Surveillance Act.

[44] Leon Spencer, *Snowden Docs Reveal NSA Digital Warfare Capabilities*, ZDNet (Jan. 19, 2015), https://www.zdnet.com/article/snowden-docs-reveal-nsa-digital-warfare-capabilities.

[45] Eileen Donahue, Hum. Rts. Watch, *Brazil as the Global Guardian of Internet Freedom?* (Feb. 13, 2015), https://www.hrw.org/news/2015/02/13/brazil-global-guardian-internet-freedom.

[46] *See, e.g.*, Damian Paletta, *How the U.S. Fights Encryption—and Also Helps Develop It*, Wall St. J. (Feb. 22, 2016), https://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096.

The harm to internet freedom from the Snowden and related disclosures went beyond mere revelations of U.S. hypocrisy. The disclosures chilled certain forms of online communications for fear of government snooping.[47] Most significantly, they gave nations a powerful incentive and a powerful excuse to exert more control over their domestic networks in response to perceived U.S. cyber incursions, along with a roadmap for doing so.[48]

II. Failure Abroad

By the time that Secretary Clinton began to speak about internet freedom, a decade after Bill Clinton's presidency had ended, China was doing a pretty good job of nailing the Jell-O of undesirable speech to the wall of Party control. Some in 2010 still had doubts that China would succeed. Today, five years after Snowden's revelations, China is approaching mastery over the internet communications that it cares most about, which are mainly forms of organizational speech and collective expression that it believes threaten the Party and public order generally.[49]

China has established digital filters at the border that allow in only the types and quantities of information the Party wants. CNN, ESPN, and the *Washington Post* can currently be accessed in China, but Facebook, Google, YouTube, Twitter, and Instagram are blocked and replaced by home-grown and government-friendly substitutes that flourish behind the Great Firewall.[50] China has also been tightening its grip on the "virtual private networks" that allow sophisticated users to defeat these filters.[51]

Inside the country, an intricate regime of surveillance, counter-speech, censorship, and targeted disruption enables additional Party control, often in real time.[52] These tools are supported by a deterrence strategy of prominent arrests, fines, extralegal detentions, and forced confession for writers, journalists, and dissidents who violate China's speech rules. China has also been developing a real-name identity registration system to prevent

---

[47] *See, e.g.*, Alex Marthews & Catherine Tucker, Government Surveillance and Internet Search Behavior (Feb. 17, 2017) (unpublished manuscript), https://ssrn.com/abstract=2412564; Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech. L.J. 117 (2016); Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 Journalism & Mass Comm. Q. 296 (2016).

[48] In addition to the developments recounted in Part II below, see, for example, Ron Deibert, *The Geopolitics of Cyberspace After Snowden*, Current History, Jan. 2015, at 9; Asaf Lubin, *A New Era of Mass Surveillance Is Emerging Across Europe*, Just Security (Jan. 9, 2017), https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe; Charles Maynes, *Snowden Revelations Lead Russia to Push for More Spying on Its Own People*, PRI (Dec. 4, 2013), https://www.pri.org/stories/2013-12-04/russia-uses-snowden-excuse-step-spying-its-own-people; Tatevik Sargsyan, *Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security*, 10 Int'l J. Comm. 2221 (2016).

[49] *See* Gary King et al., *How Censorship in China Allows Government Criticism but Silences Collective Expression*, 107 Am. Pol. Sci. Rev. 1 (2013).

[50] *See* Furio Fu, *The List of Blocked Websites in China*, Sapore di Cina (Jan. 10, 2018), https://www.saporedicina.com/english/list-of-blocked-websites-in-china.

[51] *See* Radio Free Asia, *China to Block Overseas VPN Services from End of March* (Jan. 31, 2018), https://www.rfa.org/english/news/china/china-to-block-overseas-vpn-services-from-end-of-march-01312018102313.html.

[52] *See, e.g.*, Simon Denyer, *China's Scary Lesson to the World: Censoring the Internet Works*, Wash. Post (May 23, 2016), https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html; Simon Denyer, *The Walls Are Closing In: China Finds New Ways to Tighten Internet Controls*, Wash. Post (Sept. 27, 2017), https://www.washingtonpost.com/world/asia_pacific/the-walls-are-closing-in-chinafinds-new-ways-to-tighten-internet-controls/2017/09/26/2e0d3562-9ee6-11e7-b2a7-bc70b6f98089_story.html; John Leonard, *China's Great Firewall: How It Works and What It Reveals About China's Plans*, V3 (Apr. 23, 2018), https://www.v3.co.uk/v3-uk/analysis/3030741/chinas-great-firewall-how-it-works-and-what-it-reveals-about-chinas-plans.

anonymity and to enhance surveillance, as well as a related "social credit system" that (among many other things) seeks to tie online access to online behavior.[53] And China requires foreign and domestic firms to keep the "critical information infrastructure" they collect inside China and to give the government access for security purposes.[54] Apple is typical among U.S. firms in complying with China's law enforcement and security demands, even as it has resisted in court several U.S. government efforts at cooperation on law enforcement.[55]

A core assumption of the U.S. internet freedom agenda is that online censorship and control retard innovation and modernization. "[C]ountries that restrict free access to information or violate the basic rights of internet users risk walling themselves off from the progress of the next century," Clinton warned China and other authoritarian states in her 2010 speech.[56] China is in the process of proving this assumption false. It is creating an internet that reflects the Party's values and protects its interests. At the same time, China permits its nearly 800 million internet users to communicate with each other and the rest of the world on a vast array of topics. It also fosters a sophisticated and robust e-commerce space, led by Chinese companies that include four of the world's largest internet firms: Alibaba (online shopping), Baidu (search), Tencent (social media and messaging), and Xiaomi (smartphones and related products). China has a vibrant technology start-up scene that is starting to rival Silicon Valley's.[57] It is probably ahead of the United States in digital payment systems, mobile commerce, and next-generation wireless technology, and it appears to be holding its own in the important fields of artificial intelligence and quantum computing.[58] Its technology firms, meanwhile, are making the turn from copycats to innovators and are starting to compete abroad, especially in Asia.[59]

The U.S. government has been unable to stymie China's singular approach to mixing political control and commercial freedom on the internet. Since Snowden destroyed its remaining moral leverage and Donald Trump became president, it has practically stopped trying. Access to China's gargantuan market is so cherished by American firms that they acquiesce in policies of government intrusion and surveillance they would not tolerate in

---

[53] *See* Chris Mirasola, *Understanding China's Cybersecurity Law*, Lawfare (Nov. 8, 2016), https://www.lawfareblog.com/understanding-chinas-cybersecurity-law; Samm Sacks & Paul Triolo, *Shrinking Anonymity in Chinese Cyberspace*, Lawfare (Sept. 25, 2017), https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace.

[54] *See* Chris Mirasola, *China's New Guidance Further Restricts the Transfer of Digital Information*, Lawfare (Apr. 17, 2017), https://www.lawfareblog.com/chinas-new-guidance-further-restricts-transfer-digital-information.

[55] *See, e.g.*, Tim Bradshaw, *Apple Drops Hundreds of VPN Apps at Beijing's Request*, Financial Times (Nov. 21, 2017), https://www.ft.com/content/ad42e536-cf36-11e7-b781-794ce08b24dc; Stephen Nellis & Cate Cadell, *Apple Moves to Store iCloud Keys in China, Raising Human Rights Fears*, Reuters (Feb. 24, 2018), https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060.

[56] Clinton, *supra* note 10.

[57] *See* Phred Dvorak & Yasufumi Saito, *Silicon Valley Powered American Tech Dominance—Now It Has a Challenger*, Wall St. J. (Apr. 12, 2018), https://www.wsj.com/articles/silicon-valley-long-dominated-startup-fundingnow-it-has-a-challenger-1523544804; Joanna Glasner, *US Early-Stage Investment Share Shrinks as China Surges*, TechCrunch (Apr. 16, 2018), https://techcrunch.com/2018/04/16/us-early-stage-investment-share-shrinks-as-china-surges.

[58] *See, e.g.*, *America v China: The Battle for Digital Supremacy*, Economist (Mar. 15, 2018), https://www.economist.com/news/leaders/21738883-americas-technological-hegemony-under-threat-china-battle-digital-supremacy; *In Fintech, China Shows the Way*, Economist (Feb. 25, 2017), https://www.economist.com/news/finance-and-economics/21717393-advanced-technology-backward-banks-and-soaring-wealth-make-china-leader; Gabriel Wildau & Leslie Hook, *China Mobile Payments Dwarf Those in US as Fintech Booms, Research Shows*, Financial Times (Feb. 13, 2017), https://www.ft.com/content/00585722-ef42-11e6-930f-061b01e23655.

[59] *See China's Internet Giants Go Global*, Economist (Apr. 20, 2017), https://www.economist.com/business/2017/04/20/chinas-internet-giants-go-global.

the United States. The U.S. government has, in turn, tolerated this acquiescence, perhaps because it realizes that too much pressure on Beijing over censorship would result in retaliation that would harm American companies and the American economy on balance. American efforts to introduce digital tools to defeat China's control over the political aspects of its internet have also failed. Proposals to invoke international trade law to fight back against what the United States sees as the digital protectionism of the Great Firewall have gone nowhere and are unlikely to succeed even if pursued with more vigor.

China is an extreme case. At the dawn of the Arab Spring, it seemed that the internet, especially social media platforms such as Twitter, YouTube, and Facebook, had a better chance of fostering freedom in Arab nations. Many of the leaders of the 2010–2011 uprisings in Tunisia, Libya, Egypt, Yemen, Syria, and Bahrain were trained to use digital technologies by organizations sponsored by the U.S. government and U.S. internet firms. But whatever advantages these technologies initially brought—a debated point—they now appear to have been reversed. The communications tools that seemed to mark a decisive advantage against Arab governments reflected only a temporary advantage due to government incompetence and inattention. In the last five years, authoritarian Arab regimes have reasserted control. They have done so by using tanks, to be sure. But they have also begun to master digital technologies and to deploy them to censor, surveil, and disrupt protesters and to actively cultivate alternative nationalist movements using "bots" and armies of fake users. "The very technologies that many heralded as 'tools of liberation' . . . are now being used to stifle dissent and squeeze civil society," Ron Deibert has observed.[60] These governments have also grown adept at employing internet shutdowns and slowdowns, at blocking encrypted communication tools, and at cracking down on circumvention efforts.

The trend of increasing internet control by governments extends beyond China and the Arab states. In 2009, Freedom House initiated an annual global survey of internet freedom that measured national limits on internet content, internet access, and violations of user rights, including undue surveillance, privacy violations, and penalties for online speech. Its 2017 report found that internet freedom, so measured, was becoming increasingly precarious. "Disinformation tactics contributed to a seventh consecutive year of overall decline in internet freedom, as did a rise in disruptions to mobile internet service and increases in physical and technical attacks on human rights defenders and independent media," Freedom House concluded.[61] "A record number of governments have restricted mobile internet service for political or security reasons, often in areas populated by ethnic or religious minorities," and "[g]overnments around the world have dramatically increased their efforts to manipulate information on social media over the past year."[62]

It is not just authoritarian nations that have defied American-style internet freedom. In recent years, the nations of the European Union have come to see the hegemony of U.S. internet firms as nothing less than a danger to the European way of life. In part, this is due to the revelation that the NSA had been sucking up massive amounts of data about European citizens initially collected by U.S. firms. And in part, it is because U.S. internet firms wield their enormous power to shape morals, politics, news, consumer choice, and much more in ways that many European officials abhor. "We are afraid of Google" because it threatens "our values, our understanding of

[60] Ron Deibert, *Authoritarianism Goes Global: Cyberspace Under Siege*, J. Democracy, July 2015, at 64, 64.
[61] Freedom House, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy* (2017), https://freedomhouse.org/report/freedom-net/freedom-net-2017.
[62] *Id.*

the nature of humanity, our worldwide social order and, from our own perspective, the future of Europe," wrote Mathias Döpfner, the CEO of Axel Springer SE, Germany's largest media group, in a much-noted open letter to Google CEO Eric Schmidt in 2014.[63] In recent years, European regulators have embraced this philosophy and significantly ramped up their legal pressure of American technology firms. Many believe that this pressure is motivated in part by economic protectionism.[64] Perhaps so. The point for now is that Europe's internet regulators are becoming more active within European borders, and sometimes beyond.

European regulators have, for example, fined Google $2.7 billion for abusing its economic power in the arena of internet search and Apple $15.3 billion for unpaid taxes.[65] Several other antitrust investigations against Google and other U.S. tech firms are in the works, and European regulators are searching for ways to impose billions more in taxes. They have also threatened these firms with severe sanctions if they do not clamp down on hate speech, incitement, and terrorist violence. They have recognized a "right to be forgotten," which allows individuals to remove detrimental personal information from search results on the web—not just in Europe but possibly everywhere in the world. European courts, alarmed by the Snowden revelations, have raised the privacy bar for sending data collected in Europe to the United States, for fear of NSA snooping. And most significantly, the new General Data Protection Regulation (GDPR) in Europe imposes burdensome new data disclosure and privacy rules for firms handling the information of EU citizens.[66] These rules are in the process of being adopted by firms globally, including in the United States.[67]

The GDPR is one of scores of recent national and regional regulations related to privacy, security, surveillance, and law enforcement that limit the flow of information across national borders and pressure firms to store data about users in a given country on servers located within that country.[68] Other non-tariff barriers to digital free trade that have grown sharply in recent years include local infrastructure or computing requirements, local partnership requirements, intellectual property infringement, cross-border cybertheft, and the various means of filtering and blocking information from abroad noted above.[69] The United States has gotten in the game, mostly through an interagency committee to review foreign investments known as the Committee on Foreign Investment in the United States (CFIUS). CFIUS now regularly flouts the commercial non-regulation principle with its aggressive

[63] Mathias Döpfner, An Open Letter to Eric Schmidt (Apr. 16, 2014), *available at* http://www.axelspringer.de/dl/433625/LetterMathiasDoepfnerEricSchmidt.pdf.

[64] *See, e.g.*, Mark Scott, *E.U. Rules Look to Unify Digital Market, but U.S. Sees Protectionism*, N.Y. Times (Sept. 13, 2016), https://www.nytimes.com/2016/09/14/technology/eu-us-tech-google-facebook-apple.html.

[65] *See* Ali Breland, *Apple Pays First Batch of $15.3B Back Taxes to Ireland*, Hill (May 18, 2018), https://thehill.com/policy/technology/388359-apple-pays-first-batch-of-back-taxes-to-ireland.

[66] *See* Larry Downes, *GDPR and the End of the Internet's Grand Bargain*, Harv. Bus. Rev. (Apr. 9, 2018), https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain.

[67] *See* Sarah Gordon & Aliya Ram, *Information Wars: How Europe Became the World's Data Police*, Financial Times (May 20, 2018), https://www.ft.com/content/1aa9b0fa-5786-11e8-bdb7-f6677d2e1ce8.

[68] For discussion of other such regulations, see Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677 (2015).

[69] *See generally* Rachel F. Fefer et al., Cong. Research Serv., R44565, *Digital Trade and U.S. Trade Policy* 12–19 (2018).

crackdown on attempts by foreign firms, notably from China, to own or control U.S. information technology firms.[70] The ostensible justification for CFIUS's growing vetoes of foreign takeovers of these firms is cybersecurity. But the trend also reflects retaliation against Chinese protectionism and worries about strategic control over crucial technology sectors.[71]

While the commercial non-regulation principle is everywhere under assault, it would be wrong to ignore its successes. The principle largely prevailed for almost two decades during which the internet boomed and large U.S. firms grabbed huge market share globally, in some instances approaching monopoly power. The United States has a big trade surplus in digital industries.[72] Both U.S. firms and U.S. consumers continue to reap the benefits of the continuing growth in the digital economy, even though U.S. firms and digital free trade are suffering pushback abroad and even though other countries and firms in other countries are catching up. It is an open question how far nations will go down the road of digital protectionism, how burdensome foreign regulations will prove to be for U.S. firms, and what impact these trends will have, especially in the burgeoning tech battle with China.

The anti-censorship principle, by contrast, is much further down the road to collapse and indeed was always a delusional goal. Nations have different values and priorities, and the American conception of freedom, especially our conception of free speech, is a global outlier. As the very different examples of China and Europe show, when the internet threatens those values and priorities, nations can preserve them by exercising sovereign muscle—brute coercive power—over local firms and communication intermediaries within their borders.[73] The internet freedom agenda never really had a plan to fight this logic. The United States lacks the economic or diplomatic power to bend China or the European Union to its will on internet matters. If anything, the dependency of American firms on access to these giant markets gives China and Europe the upper hand. Nor has the United States been able to deliver to activists abroad the digital tools to defeat control in weaker nations, which have largely succeeded in reversing the impact of these tools for their own ends.

III. Failure at Home

The United States' internet freedom project is not just failing abroad. It is also failing at home. I explained above that the United States is increasingly engaged in forms of digital protectionism that it once decried. But both the commercial non-regulation principle and the anti-censorship principle are allowing real harms within the country's

---

[70] *See, e.g.*, *CFIUS Intervenes in Broadcom's Attempt to Buy Qualcomm*, Economist (Mar. 8, 2018), https://www.economist.com/news/business/21738398-powerful-committee-top-american-officials-becomes-more-intrusive-cfius-intervenes; Martin Giles, *CFIUS: The Powerful Sheriff Policing US Tech's Megadeal*, MIT Tech. Rev. (Mar. 9, 2018), https://www.technologyreview.com/s/610455/cfius-the-powerful-sheriff-policing-us-techs-megadeal. In recent years, CFIUS has vetoed Broadcom's attempted takeover of Qualcomm, Ant Financial's attempted takeover of MoneyGram, Fujian Grand Chip Investment Fund's attempted takeover of the U.S. business of German semiconductor company Aixtron SE, and the attempted takeover of Lattice Semiconductor by a U.S. private equity firm funded by the Chinese government.

[71] *See China's Protectionism Comes Home to Roost*, Financial Times (Jan. 3, 2018), https://www.ft.com/content/14196546-f098-11e7-ac08-07c3086a2625.

[72] *See, e.g.*, Kati Suominen, *Where the Money Is: The Transatlantic Digital Market*, Ctr. for Strategic & Int'l Stud. (Oct. 12, 2017), https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/where-money-transatlantic-digital-market ("In 2015, the U.S. had a $161.5 billion trade surplus in digitally-deliverable services.").

[73] This is the major theme of Goldsmith & Wu, *supra* note 16.

borders as well. "[M]odern information networks and the technologies they support can be harnessed for good or for ill," Clinton acknowledged in her 2010 speech.[74] The premise of the U.S. internet freedom agenda is that an open, unregulated internet is great at home on balance and thus should be exported abroad. This premise—built on an optimism about the impact of digital technologies on American public life—is now being called into question.

The first problem concerns cybersecurity. Not a week goes by without reports of major cybersecurity breaches, data thefts, information compromises, or cyberattacks in which major U.S. firms and their consumers are the victims. The U.S. government is not doing much better. A May 2018 report by the Office of Management and Budget and the Department of Homeland Security concluded that an overwhelming majority of U.S. federal agencies are ill equipped to defend their networks and cannot even "detect when large amounts of information leave their networks, which is particularly alarming in the wake of some of the high-profile incidents across government and industry in recent years."[75] The U.S. government and U.S. firms have seen this problem coming for over a decade, but they have been unable to check it. "We're the frog in the pot that's getting boiled," said Rob Joyce, the Trump administration's cybersecurity coordinator, at a conference in 2017.[76] "I watch these breaches every day," he added. "It's getting to a point where we're getting numb."[77]

Among the many reasons the United States is failing at cybersecurity is its commitment at home to the commercial non-regulation principle. Inadequate regulation is a primary cause of poor cybersecurity hygiene in the United States. Individuals have inadequate incentives to use security software and take other precautions, and firms lack proper incentives to harden their defenses and share information with each other and the government. The vast majority of software companies, internet technology firms, and individuals will not internalize the many negative cybersecurity costs they impose due to weak security standards or poor security investments unless the government provides some prodding through liability, regulation, tax incentives, standard-setting, or some other means.[78] But the United States' non-regulation commitment and concerns about the impact on innovation have significantly hampered progress on this front.

Another unfortunate side effect of internet freedom at home, and one caused more by the anti-censorship principle, is susceptibility to information operations from abroad. Explaining the difficulty of preventing Russia from stealing emails from Democratic National Committee (DNC) accounts, President Obama explained shortly before leaving office that "our economy is more digitalized and it is more vulnerable, partly because . . . we have a more opened society and we are engaged in less control or censorship[] over what happens on the internet."[79] The United States has a wider and more readily accessible digital attack space than any nation in the world, and much of this attack space lies in the private sector, including private channels of communication. The U.S. commitment

[74] Clinton, *supra* note 10.
[75] Exec. Office of the President, *Federal Cybersecurity Risk Determination Report and Action Plan* 15 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf.
[76] Gus Hunt, *Cyber Moonshot: The Time Has Come*, Accenture Security Blog (Oct. 24, 2017), https://www.accenture.com/us-en/blogs/blogs-cyber-moonshot-time-come.
[77] *Id.*
[78] *See, e.g.*, Tyler Moore, *The Economics of Cybersecurity: Principles and Policy Options*, 3 Int'l J. Critical Infrastructure Protection 103 (2010).
[79] *Full Transcript: President Obama's Final End-of-Year Press Conference*, Politico (Dec. 16, 2016) [hereinafter Obama Transcript], https://www.politico.com/story/2016/12/obama-press-conference-transcript-232763.

to free speech, relative anonymity, and sharp limitations on domestic government surveillance—all virtues from a civil liberties perspective, of course—makes it hard for our government to identify, prevent, and respond to malicious cyber operations, especially ones that seek to manipulate information for nefarious ends. This is the very problem of social disruption and instability from online foreign meddling that Russia and China have been harping about, and taking steps to check, for years.

Another way in which internet freedom threatens American institutions is in the pathological forms of speech that it fosters. There are many reasons for the political and social fracturing of American society, but arguably near the top of the list is the balkanization of information consumption, and the attendant coarsening of public discourse, that digital technologies foster. The internet, and especially social media platforms such as Facebook and Twitter, promote the sort of fine-grained, self-serving, and exclusionary information consumption that Cass Sunstein has called "self-insulation."[80] As Sunstein and others have argued, self-insulation makes it harder to empathize with citizens whose concerns and opinions differ; enhances mutual alienation, misunderstanding, and polarization; and subsidizes the spread of falsehoods, conspiracies, and counterfeit news. The internet has also enabled a proliferation of specialty news and information sites that tend to be more extreme and partisan than traditional "meat-space" media and that intensify self-insulation, especially in a heterogenous society like the United States. All these tendencies have a devastating impact on our deliberative democracy, which depends for its success on mutual understanding, compromise, and learning.

A final problem comes in the form of the weaponization of speech.[81] The internet has made speech cheap to produce and to aggregate. This has allowed private actors to engage in vicious group attacks by "troll armies" that aim to discredit or to destroy the reputation of disfavored speakers and to discourage them from speaking again. A related practice is to distort or overcome disfavored speech by using fake news, fake commentators, and other forms of misinformation or propaganda to muffle the disfavored speech or confuse the audience. Both practices take advantage of the pathologies of self-insulation. And the impact of both can be magnified by bots that automatically send and resend the weaponized speech on a large scale. The aim of weaponized speech is often to create a fog that prevents all news sources, and all informed critical commentary, from being trusted.

These maladies of internet freedom at home converged in the historic event that may one day be seen as its death knell: the Russian information operation in the presidential election of 2016. In 2010, Hillary Clinton spoke of internet freedom as a means to end censorship and control in authoritarian nations like Russia. Six years later, such efforts had had no apparent effect on that country. On the contrary, Russian president Vladimir Putin, perhaps in response to perceived provocations by Clinton,[82] was able to exploit internet freedom and openness in the United States to cause unprecedented disruption in its democratic processes, possibly denying her the presidency. The DNC hack, as President Obama noted, was "not particularly sophisticated—this was

[80] *See, e.g.*, Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* 252 (2017) (stressing "the serious problems for individuals and societies alike that are likely to be created by the practice of self-insulation").

[81] For a good summary, see Tim Wu, Knight First Amendment Inst., *Is the First Amendment Obsolete?* (2017), https://knightcolumbia.org/sites/default/files/content/Emerging%20Threats%20Tim%20Wu%20Is%20the%20First%20Amendment%20Obsolete.pdf.

[82] *See* Fiona Hill, *3 Reasons Russia's Vladimir Putin Might Want to Interfere in the US Presidential Elections*, Vox (July 27, 2016), https://www.vox.com/2016/7/27/12304448/putin-elections-dnc-hack; Josh Meyer, *DNC Email Hack: Why Vladimir Putin Hates Hillary Clinton*, NBC News (July 26, 2016), https://www.nbcnews.com/news/us-news/why-putin-hates-hillary-clinton-n617236.

not some elaborate, complicated espionage scheme."[83] It was a simple phishing operation that extracted email messages which, once made public and churned through social media, caused a public storm. The Russians also weaponized speech through social media accounts in ways that appeared to be designed to advantage Donald Trump. For many Americans, these commonplace tactics called into question the legitimacy of the election and of the democratic system more broadly. The really bad news is that there is little to prevent something like this, or worse, from happening in the next presidential election, this time at the hands of multiple foreign actors.

Conclusion: Tradeoffs

The Trump administration has hollowed out the State Department and has deemphasized human rights and free trade. It is thus doubtful that it will give much support to the internet freedom agenda. But even a future administration more sympathetic to the agenda will need to address its failures to date by acknowledging some uncomfortable realities about the internet and by facing some large tradeoffs. Here are what I think are the three most important ones.

The first set of tradeoffs arise from how the United States promotes its anti-censorship principle abroad. That principle is premised on a commitment to spreading democracy and U.S. constitutional values that has been a lynchpin of American foreign policy since at least World War II, if not earlier. There are many ways to maintain this commitment while rethinking the tactic of meddling in foreign networks to undermine authoritarian governments. The American people are angry about and threatened by Russian cyber interference in the 2016 election. But the Russian government, as well as China's and Iran's governments and others, are angry about and threatened by U.S. intervention in their domestic networks with the ultimate aim of changing their forms of state and society.

Network interventions to promote freedom and democracy are not on the same moral plane as network interventions to disrupt or undermine democracy. But regardless of the morality of the situation, it is fanciful to think that the digitally dependent United States can continue its aggressive cyber operations in other nations if it wants to limit its own exposure to the same.[84] Unless the United States can raise its cyber defenses or improve its cyber deterrence—a dim prospect at the moment—it will need to consider the possibility of a cooperative arrangement in which it pledges to forgo threatening actions in foreign networks in exchange for relief from analogous adversary operations in its networks.[85] The Russian government recently proposed a mutual ban on foreign political interference, including through cyber means.[86] The significant hurdles to such an agreement include contestation over the terms of mutual restraint, a lack of trust, and verification difficulties.[87] These high

[83] Obama Transcript, *supra* note 79.

[84] *See* Jack Goldsmith, *Contrarian Thoughts on Russia and the Presidential Election*, Lawfare (Jan. 10, 2017), https://www.lawfareblog.com/contrarian-thoughts-russia-and-presidential-election.

[85] *Id.*

[86] *See* John Hudson, *How Putin Hoped to Make Up with Us*, BuzzFeed News (Sept. 12, 2017), https://www.buzzfeed.com/johnhudson/russia-sought-a-broad-reset-with-trump-secret-document-shows?utm_term=.rgYVRpVOg#.gcO9oA96y; John Hudson, *No Deal: How Secret Talks with Russia to Prevent Election Meddling Collapsed*, BuzzFeed News (Dec. 8, 2017), https://www.buzzfeed.com/johnhudson/no-deal-how-secret-talks-with-russia-to-prevent-election?utm_term=.lbWRAplgn#.nymEA2r3o.

[87] *See* Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, Hoover Inst. (Mar. 9, 2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf; Jack Goldsmith, *On the Russian Proposal for Mutual Noninterference in Domestic Politics*, Lawfare (Dec. 11, 2017) [hereinafter Goldsmith, *On the Russian Proposal*], https://www.lawfareblog.com/russian-proposal-mutual-noninterference-domestic-politics.

hurdles are not obviously higher than the hurdles to improving U.S. cyber defenses and cyber deterrence. And yet, no one in the U.S. government appears to be thinking about which sorts of operations the United States might be willing to temper in exchange for relief from the devastating cyber incursions of recent years.[88]

The second set of tradeoffs concern U.S. skepticism about more extensive government regulation of, and involvement in, domestic networks. The devastating cyber losses that the United States has been suffering result in large part from market failures that only government regulation can correct. The government will also need to consider doing more to police and defend telecommunications channels from cyberattack and cybertheft, just as it polices and defends threats that come via air, space, sea, and land. This might involve coordination with firms to scan internet communications, to share threat information, and to frame a response. And it might require accommodations for encrypted communications. The hazards for privacy from these steps are so extreme as to make them seem impossible today. But there are also serious hazards for privacy from not providing adequate cybersecurity.[89] If the threat to our valuable digital networks becomes severe enough, the American people will insist that the government take steps to protect them and the forms of social and economic life they enable. Our conception of the tradeoffs among different privacy commitments and between privacy and security will adjust.

Finally, U.S. regulators, courts, and tech firms may need to recalibrate domestic speech rules. Tim Wu has recently proposed some ways to rethink First Amendment law to deal with the pathologies of internet speech.[90] For instance, First Amendment doctrine might be stretched to prevent government officials from inciting attack mobs to drown out disfavored speakers, as President Trump has sometimes appeared to do. Or the doctrine might be tempered, to allow the government to more aggressively criminalize or regulate cyberstalking and trolling, or even to require speech platforms to provide a healthy and fair speech environment. These are bold reforms, but they are also potentially very dangerous. The line between genuine political speech (including group speech) and propaganda and trolling will be elusive and controversial. The effort to ensure a healthy speech environment is even more fraught and will invariably ban or chill a good deal of speech that should be protected. These misgivings do not mean that such modifications are not worth exploring or that current understandings of the First Amendment are sacrosanct. They just mean that here, as with the other tradeoffs, the choices we face are painful.

---

[88] *See* Goldsmith, *On the Russian Proposal*, *supra* note 87.

[89] *See* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. Chi. L. Rev. 221, 235–36 (2016). For an argument that encryption backdoors and related proposals are bad for all stripes of privacy, including privacy compromised by bad cybersecurity, see Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (2017).

[90] Wu, *supra* note 81, at 19–26.