# TO BE CONTINUED: TECHNOLOGY POLICY IN THE FIRST HUNDRED DAYS

*Derek E. Bambauer*[*]

## INTRODUCTION

Technology policy issues were a dominant theme in the 2020 presidential election campaign between then-President Donald Trump and former Vice President Joseph Biden. The contest was in many ways the salad days for Internet law scholars and wonks. Those seeking near-constant, unpredictable developments in technology policy must have been disappointed by the election's outcome. Now-President Biden has taken a steady, incremental approach to the formation and rollout of his technology initiatives, to the degree that his priorities still remain somewhat inchoate. However, four trends have tentatively emerged. First, as part of his infrastructure investment efforts, President Biden is pushing for further deployment of broadband Internet capabilities, especially for people in remote areas or who lack the resources to procure high-speed access through the private market. Second, President Biden's appointments herald a sea change in the federal government's approach to antitrust doctrine and enforcement. Hipster antitrust is upon us. This shift will produce lively debate, but its ability to generate meaningful results is in doubt. Third, while the role of major Internet platforms such as Facebook, Twitter, and Amazon will continue to generate headlines, legislative reform of how these companies moderate content (such as changes to Section 230) is increasingly unlikely. Finally, cybersecurity challenges—in particular, from nation-states such as China and Russia—have immediately put the new administration's national security and technology savvy to the test. While security contests are largely waged in the shadows, there are encouraging signs that Biden's team will devote the focus, resources, and patience necessary to improve America's information infrastructure.

In short, President Biden's technology efforts in his first hundred days in office have been relatively modest, and are likely to remain so given his focus

* Professor of Law, University of Arizona James E. Rogers College of Law. I thank Dan Hunter, Gus Hurwitz, Gondy Leroy, Jason Mazzone, Gavin Milczarek-Desai, Thinh Nguyen, Sergio Puig, Shalev Roisman, Allan Sternstein, David Thaw, Charlotte Tschider, and Alan Trammell for helpful suggestions and discussion. I welcome comments at <derekbambauer@email.arizona.edu>.

on the novel coronavirus pandemic, on achieving bipartisan support for his initiatives, and on incremental change. But, as his cybersecurity work demonstrates, the first hundred days is an imperfect prologue, which deserves to be titled: To Be Continued.

## I. BETTER PIPES

The crisis produced by the COVID-19 virus in early 2020 placed many Americans in near-complete isolation, sheltering in place to avoid contracting—or spreading—the pandemic. A large fraction of economic activity suddenly went online, from education to entertainment. Americans held business meetings over Zoom, caught up with loved ones over FaceTime, and whiled away pandemic evenings with Netflix. More than ever, the country depended upon broadband. That reliance exposed the depth of the digital divide. Although accurate data is difficult to obtain (especially after Trump's Federal Communications Commission (FCC) moved the goalposts to generate a Potemkin village of impressive broadband deployment), roughly a third of rural Americans do not have access to a single high-speed Internet provider. For those who can buy broadband, prices can be prohibitive, particularly given that most of the country faces either monopoly or duopoly supply. As broadband became the gateway to school, work, and social life, high-speed Internet changed from a luxury to a necessity.

Candidate Biden promised to reduce the digital divide by investing in both wired and wireless infrastructure. As Vice President, Biden was part of the Obama administration's stimulus efforts that included $4.7 billion dollars for high-speed Internet access deployment under the Broadband Technology Opportunities Program (BTOP). Biden's approach differs, though, in that his proposal expressly contemplates building government-owned infrastructure, such as municipal broadband, alongside grants to private telecommunications companies to deploy high-speed connections. And, the administration's buildout plan concentrates on networks run by public entities such as local governments, non-profit organizations, and co-operatives. It overtly supports municipal broadband, in sharp contrast to Republican-led opposition to it. Candidate Biden drew parallels between the Depression Era project of creating nationwide, ubiquitous access to electricity and his platform for broadband deployment. In his first hundred days, President Biden has proposed devoting $100 billion over eight years to rural broadband, along with rollout of emergency broadband subsidies and improved mapping of broadband deserts by the FCC. If God is in the details, then the Biden administration is trending towards divinity by including provisions for critical but oft-overlooked points like providing access to federally-owned resources such as telephone poles and rights of way. Small things make a difference when it comes to increasing competition.

The poor and the digital divide will always be with us. But, the Biden administration's plan to spur broadband deployment is an encouraging mixture of pragmatism and federal government investment that should pay dividends even after Americans are comfortable with returning to IRL activity.

## II. HIPSTER ANTITRUST

Antitrust law has been mostly dead for decades, under presidents from both major political parties. In recent years, antitrust enforcers have occasionally imposed conditions on mergers such as that between AOL and Time Warner, or scrutinized IBM's dominance of the mainframe computing business (that centerpiece of the gig economy), but for the most part, competition watchdogs have lain quiet. That is likely to change under the new administration, even if its antitrust leadership ultimately produces more bark than bite.

Major Internet platforms such as Google and Facebook have faced antitrust scrutiny in other jurisdictions such as the EU, and there have been increasing calls for oversight in the United States. The rise of the social media giants prompted, or at least helped hasten, the development of a new approach to antitrust matters. Termed "hipster antitrust" by former Federal Trade Commission commissioner Joshua Wright, this methodology harks back to the trustbusting days of President Teddy Roosevelt. Big is presumed to be bad. Consumer welfare is no longer the dominant criterion for evaluating mergers or other market conduct. Bright-line rules rather than standards predominate. And the hipsters have significantly more faith in the government's remedial capabilities, and expertise, than their predecessors. President Biden clearly signaled a change in course for antitrust policy by adding two of the hipster leaders, professors Lina Khan and Tim Wu of Columbia Law School, to his administration.

Reviving antitrust oversight would be a welcome development, in both analog and digital markets. The appointment of experts such as Khan and Wu lends intellectual heft to this effort. But, the administration's new street cred in antitrust faces at least two hurdles that may vitiate its initiative. First, the federal courts are comprised primarily (if not almost exclusively) of judges steeped in the prior, more cautious model of antitrust. Governmental activism in policing conduct or blocking mergers may well find a hostile reception in litigation. Even when the Department of Justice under President Bill Clinton was able to demonstrate that Microsoft abused its monopoly in the PC operating system (OS) market, its attempt to bifurcate the firm into an OS half and an applications half ran aground in the D.C. Circuit Court of Appeals.

This points up the second challenge for hipster antitrust: two-sided markets, like those in which social media platforms operate, are still poorly understood by economists and legal scholars. For consumers, most platforms feel free—they pay for usage with personal data, not with money. This presents a conundrum: if switching costs are nearly zero, how are platforms able to maintain dominance? And, if network effects and first-mover advantage are critical, what happened to Friendster, Lycos, and Google Buzz? Consumers can leave Google for Bing with a few keystrokes. And although interoperability between platforms is dubious, Facebook, Twitter, and other firms do offer APIs (Application Programming Interfaces) to those who wish to extract or examine data on them. The Supreme Court has been cautious thus far in its approach to two-sided markets, and lower courts are likely to follow that lead.

Despite these hurdles, the Biden administration's more activist approach to antitrust doctrine may produce meaningful effects. Even unsuccessful inquiries and litigation can shape the conduct of dominant firms by forcing them to divert resources, discouraging them from aggressive behavior, and emboldening competitors. Hipster antitrust may thus gain from going mainstream.

## III. REPORTS OF THE DEATH OF SECTION 230 ARE GREATLY EXAGGERATED

One of the oddities of the second half of President Trump's term was the recurring focus by the president, and then by his supporters in Congress, on a previously little-noticed statute put in place by the Telecommunications Act of 1996. Known colloquially as "Section 230," this provision provides widespread immunity from civil and even criminal actions for Internet access and application providers based upon content created by a third party. Even if Section 230 was not the prime mover in the development of the modern Internet, its protections have been invaluable to the growth of sites that feature user-generated content, including social media giants such as Twitter, Facebook, and TikTok. In many ways, Trump was the first social media president: he was highly deft in using Twitter in particular to bypass traditional journalistic gatekeepers to communicate with supporters and opponents alike.

Unfortunately, Trump's Twitter feed was a toxic mix of hate speech, appeals for violence, misinformation, and outright lies. This noxious brew created massive pressure on Twitter to act; similar postings by any other user would have certainly led to their ejection from the platform. When Twitter began to engage in fact-checking of Trump's posts, and occasionally blocking them, the former president became enraged. Someone with a bit of exposure to Internet law explained that Section 230 protected Twitter's editorial decisions (as, of course, does the First Amendment), and 230 found itself squarely and constantly in Trump's crosshairs. His continual demands to "Repeal Section 230!!!" were echoed by political fellow travelers in Congress, who put forth a wave of proposals designed to shrink or shred the law's immunities.

Oddly, Section 230's shortcomings were one of the few areas that Trump and Biden putatively agreed upon. When asked about the law during a media interview, candidate Biden simply called for its repeal, without elaboration. This seeming consensus belied critical differences in the underlying rationales for repeal espoused by the two candidates. Trump believed that platforms were censoring him and others with similar political viewpoints. Biden, and Democrats more generally, were concerned about the presence of incitement to violence, hate speech against marginalized groups, non-consensual pornography, and other suspect information distributed via Internet firms. This divergence made reform challenging if not impossible: one side wanted less censorship, and the other side more. Unlike former president Trump, President Biden does not appear to have a personal stake, or animus, about Section 230. It is simply one item on a wish list of Internet reforms. That means that Section 230 is likely to fade in visibility and importance relative to the Trump years.

When asked about Section 230, Gina Raimondo, then the nominee to lead the Commerce Department, voiced her support for altering the statute's protections to improve platforms' "accountability." Her proposal, though, suggested that the administration envisions change on a slower scale—she advocated using the National Telecommunications and Information Administration (NTIA) to convene a discussion among stakeholders about reform. Moreover, she explicitly balanced her desire for reform against the economic benefits platforms create, noting that they depend upon user-generated content for their success. Creating a stakeholder-driven process for any changes is moderate and sensible, in keeping with the overall tone of Biden's first hundred days. It is also a classic way of sidelining a controversial issue in favor of other priorities. The seeming bipartisan consensus on changing Section 230 masks deep normative differences on what the substance of reform ought to comprise. Any proposed reform would have to bridge or circumnavigate these dueling concerns—a difficult task at best, and one that the Biden administration is likely to view as a lower priority, particularly since the new president does not appear to have any personal animus towards social media.

## IV. THE CYBERSECURITY DELUGE CONTINUES

From the cybersecurity perspective, the Biden administration received a baptism by fire. The new president entered office as the SolarWinds hack came to light. Sophisticated attackers—probably part of Russia's intelligence services—were able to gain access to the networks and data of vital government agencies and major U.S.-based firms. The victims included the Department of Defense, Microsoft, Cisco, the Department of Justice, and even the Cybersecurity and Infrastructure Security Agency (CISA), a part of the Department of Homeland Security that is one of the federal government's principal cybersecurity watchdogs. While the administration quickly announced sanctions against Russia, the monumental task of assessing the damage from the attack—and remediating compromised infrastructure to keep the attackers from returning—has just begun. And while efforts focused on SolarWinds, additional hacks by Chinese attackers--of Microsoft Exchange e-mail servers[1] and the Pulse Secure virtual private network software—put additional public and private data at risk.

Cybersecurity has, in theory, been a critical national security priority for the United States since at least 1997, under administrations led by presidents from both major political parties. And yet, American cybersecurity is by consensus in a parlous state. Some of this disarray results from the inherent challenges of defending a system that is largely under private control and that faces attackers

1. Finding security vulnerabilities in Microsoft Exchange is like finding gambling in Rick's Café in "Casablanca." *See* Gabor Szathmari & Nicholas Kavadias, *How You Can Protect Your Microsoft Exchange Email Service from Cyber Attacks*, IRON BASTION (May 21, 2018), https://blog.ironbastion.com.au/protecting-microsoft-exchange-from-cyber-attacks/ [https://perma.cc/RKS4-99WV]; Lesatseaside, *Casino Gambling? I'm Shocked!*, YOUTUBE (Mar. 18, 2010), https://www.youtube.com/watch?v=SjbPi00k_ME [https://perma.cc/RPQ9-9JZN].

who possess advantages of time, numbers, and resources. At least in part, though, federal cybersecurity efforts have been woefully inadequate. Bureaucratic competition among agencies has diffused focus. Security regulation varies wildly by economic sector, and too often concentrates on procedural checklists rather than substantive precautions. The meaning of "critical infrastructure" has been watered down to the point of parody, preventing the government from concentrating on truly vital security issues.[2] Finally, cybersecurity was neglected if not outright damaged by the Trump administration (with the notable and likely inadvertent exception of CISA).

In its first hundred days, though, the Biden administration has made tentative but encouraging progress. The President has nominated or appointed experienced, technocratic leaders to positions badly in need of non-partisan expertise. He has taken steps to hold foreign countries engaged in espionage to account—a notable improvement from Trump's excuses on behalf of Russia. And, the new administration has proposed to focus its initial cybersecurity efforts on the electricity grid. Entities such as public utilities, electrical networks, and powerplants are anything but glamorous. The economic importance of the grid and power generation are hard to overstate, though, and their cybersecurity preparedness is hard to understate. Thus it is no surprise that many nightmare scenarios for security involve an attack on the power grid. The Biden team has outlined a sensible plan. It marries federal oversight with private expertise through co-regulation. CISA, with its security expertise, will partner with the Department of Energy, which has the relevant industry knowledge. The Department of Energy will promulgate a request for information to draw upon private sector insights into future security efforts for the grid. Supplying electricity is boring. The Biden administration's early cybersecurity foray can usefully help it stay that way.

## CONCLUSION

Technology policy is not at the top of the agenda for President Biden, and with good reason. But there are signs of interesting, useful activity beneath the surface, in areas such as broadband deployment that intersect critically with the new administration's efforts to tame the novel coronavirus, and in long-running efforts such as cybersecurity that could benefit from renewed focus. The early days seem promising. Stay tuned.

2. President George W. Bush's National Strategy for Homeland Security established national monuments and parks as "key assets" targeted for enhanced cybersecurity protection. *See* JOHN MOTEFF & PAUL PARFOMAK, CRITICAL INFRASTRUCTURE AND KEY ASSETS: DEFINITION AND IDENTIFICATION 8 (2004), https://apps.dtic.mil/sti/pdfs/ADA454016.pdf [https://perma.cc/CD5M-NZLG].