Sovereignty: The Race to Regulate, Putting Consumers First as Communications Technology Emerges

Symposium Authors (Multiple) *

TABLE OF CONTENTS

* This year's theme examines who would be better suited to regulate emerging technology and the related industries. For example, many states have recently passed laws regulating biometrics, driverless vehicles, and data breaches. Is Congress or the federal government better suited for this role? Conversely, should states and the federal government be left out so that the industry could develop its own standards?

Is There Freedom of Contract in the Age of Nationwide Communications Networks?

Justin Clark

When the First Responder Network Authority Board of Directors ("FirstNet") was established in 2012, Congress touted it as a way to encourage greater interconnectivity between multiple first responder agencies and facilitate communications in a time of crisis.[1] FirstNet is an independent authority within the Department of Commerce National Telecommunications and Information Administration responsible for constructing a nationwide public-safety broadband network.[2] In March 2017, FirstNet created a public-private partnership with AT&T to build out, operate, and maintain the Nationwide Public Safety Broadband Network.[3] Apart from issues of resource priority and insufficient network coverage in rural areas,[4] the very process of FirstNet's selection of a nationwide service provider has been criticized by some practitioners.[5] The chief concern with the partnership between FirstNet and AT&T is that the details of the service agreement were largely a mystery, specifically, how gaps in network coverage would be addressed by states and which types of dispute resolution mechanisms would be used between FirstNet and AT&T.[6] Although the governors of all 50 states have now accepted FirstNet's proposed partnership with AT&T,[7] the concerns around the contract negotiation process and the absence of state involvement in vetting, selection, and negotiation of service provider terms loom large

1. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-407, PUBLIC-SAFETY BROADBAND NETWORK: FIRSTNET SHOULD STRENGTHEN INTERNAL CONTROLS AND EVALUATE LESSONS LEARNED 1 (2015).

2. *See* Middle Class Tax Relief and Job Creation Act of 2012, Pub L. No. 112-96, §§ 6201-6202, 6204, 6207, 126 Stat. 156, 206, 208, 215 (2012).

3. The agreement provided that in exchange for AT&T's commitment to spend $40 billion on the project, the company would receive 20MHz of spectrum as well as payments from the government. Danny Crichton, *All 50 states vote yes on AT&T's $40 billion emergency response network FirstNet*, TECHCRUNCH (DEC. 29, 2017), https://techcrunch.com/2017/12/29/all-50-states-vote-yes-on-atts-40-billion-emergency-response-network-firstnet/.

4. *See* Stephen Klein, *Rural Response: The Need for an Effective Rural FirstNet Network*, 69 Fed. Comm. L.J. 53, 55 (2017).

5. *See* Al Catalano, *States Deserve A Complete Picture in Evaluating FirstNet/AT&T Coverage Plans, Beyond Digital Telecom Law Blog*, BEYOND TELECOM L. BLOG (June 29, 2017), https://www.beyondtelecomlawblog.com/states-deserve-complete-picture-evaluating-firstnetatt-coverage-plans/.

6. *Id.*

7. *Id.*

promising to plague future public-private partnerships in the area of spectrum development. These concerns are a further bi-product of the Federal Acquisition Regulation ("FAR"), and whether such a program should be used for other wide-scale communication projects moving forward.[8]

There are compelling arguments for why the decision on constructing a national first responder communications infrastructure should be handled through a framework like FirstNet.[9] However, the unique challenges of bringing together a myriad of law enforcement agencies at the local level, some of which have already developed their own localized system and do not have the opportunity to review the terms of the agreement, appears to create a need for a new procurement and development process.[10] The real culprit in all of this appears to be the strictures of FAR itself, a series of taxing rules governing the negotiation and administration of contracts between executive agencies and private third parties.[11] To open up negotiations and give state and local law enforcement authorities the opportunity to review the terms of a public-private partnership to develop a broad-reaching system, the FirstNet founding board might have considered using alternative means for soliciting bids and negotiating a contract. One such framework used by the Departments of Defense and Homeland Security in some of their fulfillment contracts is the "Other Transaction", an alternative instrument available for research and development efforts with certain agencies where traditional procurement laws and regulations are too burdensome.[12] Using such a regime may provide benefits in transactions involving multiple parties where cost-sharing and advancing dual-use technologies are key concerns.[13]

The creation, development, and administration of FirstNet could serve as a key lesson for other projects involving use and development of the spectrum, particularly as to how service providers are selected and how those providers negotiate contract terms with the numerous parties involved. Most importantly, Congress should consider the concerns of state and local governments and how these governments can be part of the contract negotiation and roll-out process.

---

8. *See* Al Catalano, *A Better Way Forward for FirstNet?*, BEYOND DIGITAL TELECOM L. BLOG (Mar. 8, 2017), https://www.beyondtelecomlawblog.com/better-way-forward-firstnet/.

9. "There are certainly some situations when interoperability is necessary, especially in major metropolitan areas, where first responders from multiple jurisdictions will swarm a dire emergency." *See* Steven Brill, *The $47 Billion Network That's Already Obsolete*, ATLANTIC (Sept. 2016), https://www.theatlantic.com/magazine/archive/2016/09/the-47-billion-network-thats-already-obsolete/492764/ [https://perma.cc/K8H9-2EH8].

10. Al Catalano, *States Deserve A Complete Picture in Evaluating FirstNet/AT&T Coverage Plans, Beyond Digital Telecom Law Blog*, BEYOND TELECOM L. BLOG (June 29, 2017), https://www.beyondtelecomlawblog.com/states-deserve-complete-picture-evaluating-firstnetatt-coverage-plans/.

11. Al Catalano, *A Better Way Forward for FirstNet?*, BEYOND DIGITAL TELECOM L. BLOG (Mar. 8, 2017), https://www.beyondtelecomlawblog.com/better-way-forward-firstnet/.

12. *See* Nancy O. Dix, et al., *Fear and Loathing of Federal Contracting: Are Commercial Companies Really Afraid to Do Business With the Federal Government? Should They Be?*, 33 Pub. Cont. L.J. 5, 23-7 (2003).

13. *Id.* at 26.

The How and Where of Regulating Communication Technology?

Sean Davis Jr.

In today's era, communication technology is emerging as a pillar in American society and economy. From artificial intelligence to social media platforms, tech focused companies are growing in social relevance and market space. For example, Facebook and Google, two of Silicon Valley's titans are expected to take half of the internet advertising revenue worldwide and over sixty percent in the U.S.[1] Further, with the recent rollback of open internet protections, many in congress have made net neutrality a campaign issue,[2] subsequently placing telecomm issues at the forefront of the American conscious. Other issues, such as the repeal of broadband privacy[3] begs a pertinent question: who is best suited to regulate communication technology and relevant innovations? Touching on a myriad of anti-trust and civil rights issues, technology such as social media algorithms or driverless cars creates complex legal issues that are heavily debated.

The answer to these questions although complex, are not far off. First, it is critical that regulatory bodies such as the Federal Communications Commission, the Federal Trade Commission, and the House Subcommittee on Communications and Technology acknowledge that there is a spectrum of communications technology that requires varying degrees of regulation. For example, Silicon Valley Titans such as Facebook and Google have monopolized the online advertising market[4], while subsequently being questioned for their mishandling of extremist content on their platforms[5]. Given their relevance in both American society and economy, placing sensible regulations on Facebook and Google's online advertising power and screening of user content is pertinent. On the other end, communications technology associated with artificial intelligence is in a developing stage, which would easily be stifled by too much regulation. However, there are steps that can be taken to address such tech without stifling innovation. One

1. Reuters, *Why Google and Facebook Prove the Digital Ad Market Is a Duopoly?*, FORTUNE (July 28, 2017), http://fortune.com/2017/07/28/google-facebook-digital-advertising/.

2. Klint Finley, *Why Net Neutrality will be a campaign Issue in 2018*, WIRED (Dec. 21, 2017), https://www.wired.com/story/why-net-neutrality-will-be-a-campaign-issue-in-2018/.

3. Devin Coldewey, *Broadband Privacy Rules (Update: Passed)*, TECHCRUNCH (Mar. 22, 2017), https://techcrunch.com/2017/03/22/senate-debates-legislative-rollback-of-fccs-broadband-privacy-rules/.

4. Reuters, *Why Google and Facebook Prove the Digital Ad Market Is a Duopoly?*, FORTUNE (July 28, 2017), http://fortune.com/2017/07/28/google-facebook-digital-advertising/.

5. Alex Wagner & Tony Romm, *Facebook, Google and Twitter testified before congress again*. RECODE (NOV. 21, 2017), https://www.recode.net/2017/11/1/16588374/live-updates-facebook-google-twitter-testify-senate-congress-russia-president-election.

such example is the Future of Artificial Intelligence Act of 2017. Sponsored by Senator Maria Cantwell, the Act would name the Department of Commerce responsible for creating a committee to provide recommendations on how businesses and government can come together to: (1) create reasonable legislation on artificial intelligence (AI); (2) support developmental AI ventures and protect the rights of consumers as AI continues to grow.[6] Legislation such as this shows forward thinking and recognition that communications technology is a multifaceted market that has the ability to usher the U.S. into a new economic revolution.

6. *Young Introduces bill to promote and understand the Future of Artificial Intelligence Technology.* SENATOR TODD YOUNG (Dec. 12, 2017), https://www.young.senate.gov/newsroom/press-releases/young-introduces-bill-to-promote-and-understand-the-future-of-artificial-intelligence-technology.

The Federal Trade Commission Protects Consumers as Communications Technology Evolves

Morgan Rucker Kennedy [1]

Communications technology has greatly expanded the scope of connectivity in everyday life. Consumers are no longer just connecting to the Internet through a desktop computer or home modem.[2] Instead, consumers are connecting through, among other things, mobile phones, wearables, refrigerators, thermostats, televisions, and vehicles.[3] While these technological innovations have provided revolutionary benefits to the way consumers live and interact with the people and things around them, it also means companies are collecting an immense amount of data from consumers.[4] Fitness trackers can log when you went for a walk, where you walked, your stride length, and your heart rate.[5] Modern vehicles permit you to sync your smart phone to the car's infotainment system, permitting the storage of address book, call, and text message information.[6] The amount of data collected by a potential multitude of actors means it is crucial for consumers to have transparency about companies' data use and collection practices, and confidence that their information will be kept secure.

As the leading privacy and data security agency in the United States, the Federal Trade Commission ("FTC" or "Commission") is uniquely situated to protect consumers as technology evolves. The FTC is a bipartisan independent agency with law enforcement jurisdiction over a broad swath of

1. Ms. Kennedy is an attorney in the FTC's Office of the General Counsel. The views expressed herein are the author's own and do not necessarily represent the views of the Commission or any individual Commissioner.

2. *Share of devices used to access the internet at home, in the United States, from 2010 to 2015*, STATISTA https://www.statista.com/statistics/199055/devices-used-to-access-the-internet-at-home-in-the-united-states/ (last visited Apr. 18, 2018).

3. Krissy Rushing, *5 Benefits of Internet Appliances*, http://www.hgtv.com/remodel/mechanical-systems/5-benefits-of-internet-appliance.s

4. *Connected Devices and Your Privacy*, CONSUMER REPS. (Apr. 30, 2015), https://www.consumerreports.org/cro/magazine/2015/06/connected-devices-and-your-privacy/index.htm.

5. James Stables, *Best fitness tracker guide 2018: The top activity bands you can buy now*, WAREABLE (Apr. 17, 2018), https://www.wareable.com/fitness-trackers/the-best-fitness-tracker.

6. Ronald Montoya, *Car Technology and Privacy: Top 5 Things Your Car Knows About You*, EDMUNDS (Feb. 12, 2013), https://www.edmunds.com/car-technology/car-technology-and-privacy.html.

the American economy.[7] When the FTC was founded over a century ago, Congress could not have imagined the types of technology that are commonplace in modern society. However, the FTC Act, which broadly authorizes the FTC to prevent "unfair methods of competition" and "unfair or deceptive acts or practices,"[8] gives the Commission flexibility to protect consumers as new technologies emerge.

The FTC has brought a substantial number of cases protecting the privacy and security of consumers' information, many of which have involved new or emerging technology.[9] For example, in 2013, the FTC issued a complaint against TRENDnet, Inc. ("TRENDnet"), which sold Internet-connected cameras for monitoring a user's home or business.[10] The FTC alleged that the company advertised its cameras as secure, but engaged in a number of practices that made the cameras' live feeds susceptible to unauthorized access by strangers.[11] In settling the complaint, TRENDnet was required by order to, among other things, establish and maintain a comprehensive security program designed to address security risks that could result in unauthorized access to or use of the company's devices and protect the security, confidentiality, and integrity of information collected, input into, stored on, captured with, accessed, or transmitted through the company's devices.[12] Four years later, the FTC and the Office of the New Jersey Attorney General filed a complaint alleging that VIZIO, Inc. ("VIZIO"), a manufacturer and seller of Internet-connected "smart" televisions, and an affiliated software company installed software on VIZIO televisions to collect second-by-second viewing data on millions of consumers without their

---

7. The Federal Trade Commission Act ("FTC Act") contains some limitations on the FTC's jurisdiction. The FTC Act exempts from the FTC's jurisdiction "common carriers subject to the Acts to regulate commerce," which bars the agency from reaching certain conduct by telecommunications companies. 15 U.S.C. § 45(a)(2). For well over a decade, the Commission, on a bipartisan basis, has advocated that Congress repeal this common carrier exemption. *See, e.g.*, *Prepared Statement of The Fed. Trade Commission Before the Subcomm. on Commerce, Trade, and Consumer Protection of the Comm. on Energy and Commerce* (June 11, 2003), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-reauthorization/030611reauthhr.pdf. [https://perma.cc/8TZ3-TG9S].

8. 15 U.S.C. § 45.

9. *Enforcing Privacy Promises*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Apr. 18, 2018).

10. Complaint at 2, In the Matter of TRENDnet, Inc., a Corp., No. C-4426 (FTC Sept. 3, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetcmpt.pdf. [https://perma.cc/SXA8-PLAT].

11. Complaint at 3,6, In the Matter of TRENDnet, Inc., a Corp., No. C-4426 (FTC Sept. 3, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetcmpt.pdf. [https://perma.cc/SXA8-PLAT].

12. Decision and Order, *In the Matter of TRENDnet, Inc., a Corp.*, No. C-4426 (FTC Jan. 16, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf.

knowledge or consent.[13] VIZIO and its affiliate agreed to pay $2.2 million to settle these charges, and the stipulated federal court order requires the companies to disclose and obtain affirmative express consent for their viewing data collection and sharing practices, and prohibits misrepresentations about the privacy, confidentiality, or security of consumer information collected.[14]

To pursue such matters and to police the marketplace effectively, the FTC has to remain informed about new technologies and their effects on consumers. To do so, the Agency routinely hosts workshops to engage with industry, academics, government agencies, and consumer advocates.[15] Recent workshops have examined the connected car ecosystem[16] and injury to consumers resulting from the misuse of personal information in products and services.[17] The FTC also encompasses the Office of Technology Research and Investigation ("OTech") to facilitate technical expertise internally.[18] OTech technologists conduct independent studies and assist FTC investigators and attorneys by providing technical expertise, investigative assistance, and training.[19] Finally, the FTC hears directly from the public — consumers file complaints directly with the Agency.[20] Although the FTC does not adjudicate individual complaints, it uses them to understand what practices cause significant harm to consumers and focus its investigations.[21]

For all of the above reasons, the FTC has the expertise and capability to take targeted law enforcement action to address unlawful conduct without impeding innovation.

---

13. Complaint for Permanent Injunction and Other Equitable and Monetary Relief, *FTC v. VIZIO, Inc.*, No. 17-cv-00758 (D. N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.

14. Stipulated Order for Permanent Injunction and Monetary Judgment, *FTC v. VIZIO, Inc.*, No. 17-cv-00758 (D. N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.

15. *All Events*, FTC, https://www.ftc.gov/news-events/events-calendar/all (last visited Apr. 18, 2018).

16. *Connected Cars Workshop, Staff Perspective*, FTC (Jan. 2018), https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf?utm_source=govdelivery.

17. *Informational Injury Workshop*, FTC, https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop (last visited Jan. 16, 2018).

18. *Office of Technology Research and Investigation*, FTC, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation (last visited Apr. 18, 2018).

19. *Office of Technology Research and Investigation*, FTC, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation (last visited Apr. 18, 2018).

20. *Filing A Complaint*, FTC, https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/filing-complaint (last visited Apr. 18, 2018).

21. *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FTC, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited Apr. 18, 2018).

Federal, State, and Self-Regulation Strategies for Data Collection & Use

Grant Nelson [1]

> "It is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet, . . . unfettered by Federal or State regulation; . . . ."[2]

Regulation of the collection and use of online information requires balancing the interests of encouraging technological innovation, maintaining a free and open internet, and protecting consumers' online privacy. Federal legislation, state action, and self-regulation all offer benefits and risks, and different contexts require different approaches. Ultimately, given the fast pace of technology advancement in the online information industry, a flexible approach like self-regulation may prove the most effective.

I. FEDERAL LEGISLATION

Federal legislation offers consistency across states, but not across countries, nor does it offer state-level decision-making and experimentation. Federal legislation consistency may come at the expense of the flexibility that rapidly changing technology may require. The federal legislative process takes time—so much time, in fact, that by the time a law is enacted —it may already be outdated, or is quickly made irrelevant or ambiguous by advances in technology. For example, the Computer Fraud and Abuse Act,[3] enacted in 1986 (years before home internet use—much less mobile internet use), has been called obsolete due to its dated and over-broad language.[4] Similarly, the 1986 Electronic Communications Privacy Act[5] which regulates the circumstances under which law enforcement may access electronic

1. Counsel, Compliance & Technology for the Network Advertising Initiative (NAI).
2. *See* Communications Decency Act, 47 U.S.C. § 230(b) (2016) (providing the policy reasons for protecting internet platforms and providers from being held liable as a publisher or speaker of information).
3. 18 U.S.C. § 1030 (2016).
4. *See, e.g.*, Tiffany Curtiss, *Computer Fraud and Abuse Act Enforcement: Cruel, Unusual, and Due for Reform*, 91 WASH. L. REV. 1813, 1813 (2016); Tor Ekeland, *How to Reform the Outdated Federal Anti-hacking Law*, CHRISTIAN SCI. MONITOR (Mar. 24, 2017), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0324/How-to-reform-the-outdated-federal-anti-hacking-law.
5. 18 U.S.C. § 2510 (2016).

communications without a warrant, has been criticized for using standards from "a bygone era" based on outdated technology.[6]

Amending federal statutes to account for new technology is also challenging. The Video Privacy Protection Act of 1989[7] was not amended until 2012, and even its amended form has been described by one court as "an attempt to place a square peg (modern electronic technology) into a round hole (a statute written in 1988)."[8]

Perhaps more important is the argument that legislation often has the effect of stifling innovation, a point made by many in all sectors; not just technology.[9] Regulation drives up operating costs and reduces the incentive for entrepreneurs to enter the market, thus stifling the very innovative spirit responsible for the internet as we know it today.

II. STATE LEGISLATION

State legislation creates a patchwork of regulation across the country, allowing states to "experiment" with the regulation of an industry. However, because internet companies invariably do business in all (or close to all) states, they often elect to abide by the strictest of the state laws, a practice that curtails the "experimentation" theory and often results in the same innovation-stifling effects of federal regulation. However, different states electing to take different positions with respect to technologies may encourage competition among states to attract innovative technologies.

III. INDUSTRY SELF-REGULATION

Unlike state and federal regulations, self-regulatory organizations have the ability to respond to—and even stay ahead of—advances in technology, which is a significant advantage when regulating a constantly evolving industry.[10] Perhaps more importantly, members of such associations are

---

6. Veronique de Rugy, *Federal Agencies Fight for Warrantless Access to Emails,* MERCATUS CENTER, (Aug. 13, 2015), https://www.mercatus.org/expert_commentary/federal-agencies-fight-warrantless-access-emails.

7. 18 U.S.C. § 2710 (2016).

8. Yershov v. Gannett Satellite Information Network, Inc., 104 F. Supp. 3d 135, 140 (D. Mass. 2015).

9. *See, e.g.*, Tim Day, *When It Comes to Tech, It's Regulation vs. Innovation*, U.S. CHAMBER OF COMM.: ABOVE FOLD.; https://www.uschamber.com/series/above-the-fold/when-it-comes-tech-it-s-regulation-vs-innovation (last visited Feb. 12, 2018); Andrea O'Sullivan, *Don't Let Regulators Ruin AI*, MIT TECH. REV. (Oct. 24, 2017) https://www.technologyreview.com/s/609132/dont-let-regulators-ruin-ai/; Henry I. Miller, *Bad Times Ahead for Pharmaceutical Innovation*, FORBES: OPINION (Aug. 4, 2010, 3:17PM), https://www.forbes.com/2010/08/04/fda-regulation-pharmaceuticals-opinions-columnists-henry-i-miller.html#7fb3f1306928.

10. *See generally* Robert W. Cook, *Why do we need self-regulatory organizations? - Cook*, INVESTMENT NEWS (Apr. 2, 2017), http://www.investmentnews.com/article/20170402/FREE/170409997/why-do-we-need-self-regulatory-organizations-cook.

invested in the industry's reputation, meaning their businesses benefit from both the protection of consumer privacy (thereby demonstrating to consumers that they are both professional and trustworthy), and the preservation of a free and innovative internet ecosystem.[11] As such, self-regulatory organizations craft regulations that provide meaningful consumer privacy protections, while also educating consumers and government regulators about responsible industry practices.[12] Self-regulation creates a dynamic regulatory environment in which consumers' privacy is protected, and technological innovation is encouraged.

11. *Id.*
12. *Id.*

Sovereignty Disrupted

Travis LeBlanc [1]

Sovereignty has been disrupted. Emerging technologies have repeatedly broken the molds of regulated industries such as taxicabs, hotels, telephone companies, and cable providers. At the same time as new technologies disrupt regulated industries, these same technologies are also disrupting the very regulatory processes that we have traditionally relied upon to protect the public good. The fundamental problem is the velocity of innovation has outpaced the inertia of the regulatory process. Sovereignty is at a crossroads—our system of government must quickly adapt to this new technological landscape or it will be forced to concede the "race to regulate," leaving the technology as the only contestant standing.

I. THE PROBLEM

Emerging technologies, including communications technologies, are evolving at exponential speeds and are permeating every facet of life. By 2020, it is expected that there will be between 30 and 50 billion devices connected to the internet, or about 7 for each person on the planet. Unlike the recent past where a phone was a phone, a camera was a camera, and refrigerator was a refrigerator, a phone is now a camera, a refrigerator is a television, and the coolest appliance in the house streams, listens, and talks with you. But these technologies are not simply limited to new platforms for "chatting" or "talking"; even the simplest devices that used to be "offline" products are now becoming "smart," technology-based communicators. These technologies include a long list of devices radically changing society—from smartphones to autonomous vehicles to new-fangled medical devices—whose communicative elements are essential to their nature and desirability. And many more innovations are coming down the road that we cannot yet imagine. No aspect of life or regulation will remain untouched.

Governments thus far have been unable to keep up with these technological advances, and there is no prospect of our sovereigns catching up to these rapid changes anytime soon. Our sovereigns have been unable to regulate emerging technologies effectively and timely-in part due to the velocity of innovation, the cumbersome legislative and regulatory structure

1. Travis LeBlanc is an Affiliate with the Berkman Klein Center for Internet and Society at Harvard University, an Affiliated Scholar with the Institute for Innovation Law at UC Hastings College of the Law, and a Partner at Boies Schiller Flexner LLP. Previously, Mr. LeBlanc served as the Chief of Enforcement at the Federal Communications Commission. This article has been written in Mr. LeBlanc's personal capacity. The opinions expressed in this article are his own and do not reflect the views of the Federal Communications Commission, any commissioner thereof, the federal government, or Boies Schiller Flexner.

developed in and for an offline world, the diffusion of authority across multiple government actors without a final decision maker, the lack of technological sophistication among policymakers across governments, and the comprehensiveness of the challenge in a world where everything is connected to the internet. And then there is partisan gridlock.

To be fair, states have been far better than the federal government at keeping up with technological change—they are smaller, more nimble, less gridlocked—but even they have been unable to keep up with the growth of emerging technologies. Indeed, many of these new technologies are solving problems that we traditionally relied upon the government to handle. They are providing first-class learning to students in resource-strapped schools. Ride sharing companies are solving public transportation gaps. Doctors are providing care to patients in remote areas of the country. On the media side, consumers are able to view media content anytime anywhere and to create their own high-quality content, distribute it across multiple platforms, and generate considerable revenue. As we embrace these innovations, we accept that technology can solve inefficiencies; we become more reliant upon these technologies; and we become more willing to place our trust and confidence in them as decision-making authorities.

II. THE FUTURE IS HERE

Technological innovations are not only solving public policy problems, they are also showing that they can perform existing government tasks more quickly, effectively, and at less cost-whether that is identifying perpetrators of hate crimes, evaluating which foreigners should be admitted to the country, or determining where police resources should be targeted. It is indeed beyond apparent that emerging technologies are supplanting the traditional functions of the sovereign. The advent of email largely obviated the need for a government-operated postal service. Cryptocurrencies such as bitcoin are vying to replace government-backed currencies. And elections are being influenced by social media. Fundamentally, the government is *losing* to technologists, data scientists, and machine algorithms in the race to regulate. We do not have a defined legal regime for cloud services; there are almost no laws that govern the internet of things; and digital rights are essentially non-existent or minimally enforceable. In this environment, consumers are necessarily dependent upon technologists, data scientists, and machine algorithms to protect their welfare and safety.

Yet, unlike our sovereigns, emerging technologies are not required to honor constitutional freedoms of speech, religion, and the press. Nor must they provide any kind of due process before terminating a user account, ceasing to support legacy software, or taking down user content. Nor are they bound to protect the rights to life, liberty, and the pursuit of happiness. I am by no means suggesting that technologists, data scientists, and algorithms are intending to trample on these cherished freedoms, but a lack of timely regulatory action is necessarily transforming technologists, data scientists, and algorithms into policymakers. If government does not act, we will be left

to the regulatory authority of technologists, data scientists, and algorithms—a worrisome prospect no matter how altruistic such companies may be and no matter how much these companies promise to police themselves.

Accordingly, faced with both competition from ubiquitous technology and the associated threats carried by those technologies, it is imperative we reboot our notion of sovereignty. The fundamental impact of emerging technologies on government is as tectonic as it has been in all industries. The business of regulating is no different. Just as taxi companies are reinventing themselves in the face of competition from ride sharing companies, so must the government reconsider how it regulates in the 21st Century.

The current processes of legislating and regulating are too slow and cumbersome, the legacy of a bygone offline era. As our Founding Fathers did in 1776, we must reexamine sovereignty, this time for digital life in the 21st Century. We need to hack our democracy and the regulatory process with the goal of designing a regulatory structure for a digital world. We must devise ways for governments of all levels—from state and local governments to national and international bodies—to quickly promulgate rules that are flexible and adaptable. We need our sovereigns to have the ability to regulate the problems of tomorrow rather than relegating themselves to solving the problems of yesteryear. We need our sovereigns to address a world that is constantly connected and mobile, where information and currency are not bounded by geography, and where cyberattacks may become the exception rather than rule. These are problems that the Founders of our country, even with their clairvoyant wisdom, could not have even begun to imagine. To properly address them, iterative case-by-case reforms are not enough or effective. The challenges that emerging technologies pose to sovereignty are fundamental. We must now revisit the structure of government for life in the 21st Century, the connected world we now inhabit. Sovereignty has been disrupted by emerging technologies. We cannot afford to wait. The future is already here, and it eagerly awaits governmental resolution to protect our fundamental rights.