ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

The Case for a U.S. Digital Single Market and Why Federal Preemption Is Key

ALAN MCQUINN AND DANIEL CASTRO | OCTOBER 2019

A national framework for digital economy rules would ensure the same protections for all U.S. residents, minimize transaction costs for businesses, enable opportunities to innovate, and increase efficiency in the policymaking process.

KEY TAKEAWAYS

- States and localities have created barriers to digital commerce through overlapping and conflicting rules, including in areas of data privacy and net neutrality, and Congress has failed to stop states from erecting these policies.
- A digital single market—a national market for digital goods and services free of artificial barriers and differing rules—would ensure equal protections, minimize transaction costs for businesses, and enable opportunities to innovate.
- Congress and the states should create a standard set of policies for the entire U.S. digital economy, either through cooperation between states or through federal preemption of conflicting rules.

INTRODUCTION

In today's digital world, commerce and speech are much less tied to particular geographic locations than ever before—as access to broadband is the only natural barrier to going online. Yet, governance is still tied to location. In an analog world where much of commerce was conducted locally within specific geographic boundaries, there was considerable overlap between governance and economic activity, with the latter being regulated where it was conducted. However, with the growth of the digital economy, there is a growing disjuncture between local governance and the national and international nature of the Internet. As such, when U.S. localities and states pass laws and regulations governing digital activities—including on data privacy, net neutrality, and Internet taxation—this creates a regulatory tower of Babel where firms with digital business models having to cope with a tangled amalgamate of overlapping and conflicting rules. If Congress does not become the lead authority on digital issues, the United States will lose its chance at a fully digital single market—a national market for digital goods and services free of artificial barriers—along with the significant economic and social benefits that flow from it.

The Founders understood the importance of knitting together the colonies into a more integrated market, which is why they inserted the Commerce Clause into the Constitution.[1] And indeed, for over 200 years that clause has helped the federal government and the courts ensure a more-integrated national market. But before the Internet a significant share of commerce was still local. Consumers bought products from locally owned neighborhood stores, received health care from a nearby doctor, and banked at a local financial institution. This dynamic meant that the lack of uniformity in state laws and regulations had less impact on business and the overall economy because many businesses operated in a particular state or region.

While there have long been communications technologies, such as the telegraph and telephone, that enabled cross-state commerce, the emergence of the Internet, and its evolution over the last two decades, has increased the share of out-of-state commerce. The Internet has simply made distance irrelevant for a growing share of economic activities. Consumers from Florida to Alaska shop from the same online retailers, stream movies and music from the same websites, and use the same apps to send money. The Internet has also made scale much more important to businesses, and the most successful ones are those that leverage the Internet to access as many customers as possible. This is as true for the largest Internet giants as it is for the mom-and-pop startup in a rural hamlet that has created an app it wants to sell across the nation.

In the early days of the Internet, policymakers generally recognized the growing rates of digital connectivity as a driving force for economic progress and by and large embraced a light-touch regulatory system.[2] For example, in 1996 Congress created intermediary liability rules that ensure online companies are not liable for the content posted by their users and in 1998 restricted states from imposing taxes on Internet service.[3] States also generally avoided passing rules that impacted interstate digital commerce, often only doing so as part of multi-state compacts (e.g., state electronic signature laws).[4] Congress also worked to preempt state laws restricting consumer choice in the digital market. For example, in 2003 it passed the Fairness to Contact Lens Act that gave consumers the right to their lens prescriptions wherever they lived.

As a result, many digital businesses faced few state and local barriers to operating in the United States.

But even from the beginning of the Internet era, cracks began to appear in the system. States have traditionally regulated many areas of the economy that have evolved into having nation-wide business models. For example, companies wanting to sell alcohol online nationally often found that state laws interfered with their business models.[5] Similarly, the rules for practicing law and medicine online vary from state to state, as do the regulations for online gambling.[6] As more parts of the economy have become digital, state-based regulation has become a growing impediment to a U.S. digital single market.

Many state and local legislators no longer feel a need to employ a light-touch approach to Internet policy or to avoid creating their own unique set of rules.[7] They are no longer afraid of "breaking the Internet." There are many reasons for this change. Some lawmakers feel emboldened by a growing "techlash"—the growing animosity against technology and the companies that offer it. Some feel, rightly so in some cases, that Congress has not done enough to address problems and thus it is up to the states to intervene. Others argue they are closer to their constituents and thus more attuned to their needs than more distant federal legislators. Moreover, states often see themselves as "laboratories of democracy," a phrase coined by Supreme Court Justice Louis Brandeis to describe how states try novel policy experiments that, if successful, can be adopted by their counterparts and even the national government.[8] These factors mean that lawmakers are now much more willing to enact rules for the online economy without regard to what other states are doing, creating a thicket of regulations that make it much more difficult and costly for firms, especially small and mid-sized firms, to offer products and services online.

Multiple jurisdictions have the ability to set laws affecting activity the Internet. But if every jurisdiction imposed its own set of rules, most companies would find it burdensome to do business online, especially if these rules are not uniform. To avoid this problem, there have been various attempts at the international and national levels to harmonize rules impacting different sectors of the global digital economy. At the international level, the United States has sought to reduce digital regulatory conflicts with other countries through its trade deals. For example, the United States-Mexico-Canada Agreement (USMCA) seeks to harmonize rules across each of the various jurisdictions.[9] Likewise, the European Union has undertaken a major initiative to establish a "digital single market," which would harmonize many laws affecting digital products and services, including those on consumer protection, contracts, copyright, telecommunications, and cross-border taxes.[10] EU officials have recognized that a major factor holding Europe back from not only wider digital adoption but also the creation of more globally competitive companies with Internet-based business models is the patchwork of different laws and regulations across the European Union. While Europe has made considerable progress, it still has a long way to go, in part because national governments continue to resist EU-wide harmonization (see Box 1).[11]

While EU officials understand the importance of creating a digital single market and are taking needed steps in that direction, the United States is going in the opposite direction. Many states have already created conflicting rules, including California with its new privacy law, and many more are seeking to add their own rules.[12] For example, many states have their own unique data-

breach notification laws. Certainly, one reason why some states have acted is because the federal government has not.

Another motivation for states to erect their own regulations is to protect domestic "bricks and mortar" firms from out-of-state digital competitors. For example, several state governments blocked Tesla from opening stores in their jurisdictions to sell cars directly to consumers due to anti-competitive laws that required consumers to buy through incumbent third-party car dealerships.[13] States have also passed laws making it harder for companies to sell a variety of good and services online, including contact lenses, real estate, wine, human resources services, and more, all strongly supported by incumbent businesses and professions seeking to be sheltered from competition. These efforts ultimately raise costs, limit innovation and reduce welfare for consumers, who must pay more for services or lose access to them entirely.[14] This regulatory patchwork imposes higher compliance costs on companies, making it more difficult, time consuming, and costly for companies, especially smaller firms and startups, to scale services to the entire United States.[15] And when multiple states are creating laws and regulations on the same issue area, companies operating in those states must engage in policy debates in each state to ensure their interests are not overlooked—an expensive undertaking.

There should be wide agreement that national rules are better than individual state rules for policies that impact the U.S. digital economy.

Regardless of the rationale for any state to reason for its position on a particular policy issue, there should be wide agreement that national rules are better than individual state rules for policies that impact the U.S. digital economy. There is little reason to create one level of protections for the online privacy and security of residents of Florida and a different one for residents of Alabama. It is time for Congress, which is empowered by the U.S. Constitution to be the arbitrator of interstate commerce, to step in and create a U.S. digital single market by preempting states from erecting barriers in the U.S. digital economy.[16] A single, common framework with clear obligations can reduce burdens on existing companies, lower entry costs for new firms, and bring greater transparency to crucial, contested policy questions. This report will show that the United States lacks a digital single market and make the case for why Congress should change that. It will then outline steps Congress can take to address this challenge.

THE U.S. DOES NOT HAVE A DIGITAL SINGLE MARKET

The U.S. federal system of government empowers states and localities to create rules affecting those within their borders, while the national government helps manages interstate issues. This system is supposed to ensure a healthy division of labor, with each level of government doing what it does best. Unfortunately, it has increasingly led to siloed regulations as states legislate in conflicting ways and the federal government fails to act to prevent the resulting economic barriers. There are several categories of these barriers to digital commerce.

First, each state may have its own business and professional licensing requirements. Having to be licensed in multiple states increases the cost of businesses offering services across state lines. For example, states have created complex licensing regimes for telehealth providers, payment companies, insurance companies, and more—which often makes it very difficult for

companies using digital business models to scale up. These restrictions are often targeted at Internet companies.

Second, states create conflicting rules that increase the cost of companies doing business in multiple states. Take, for example, state data-breach notification laws, which require organizations to notify individuals (or regulators) when their personal information has been exposed. The goal of notification is to give affected individuals the opportunity to take actions to protect themselves against identity theft or fraud as well as to create market pressures on companies to improve their information security practices. Unfortunately, in the absence of a uniform federal standard, states have passed mismatched and expanded data breach requirements.[17] The lack of a uniform federal standard has created both a siloed market, where not all users are covered, and an unnecessarily complex situation for companies, which must now spend more time navigating this murky legal terrain that could be better spent protecting consumer data. States have also considered mismatched measures for other data security issues, such as mandating backdoor access to encrypted devices. For example, a bill introduced in California in 2016 would have required that any smartphone sold in the state be "capable of being decrypted and unlocked by its manufacturer or its operating system provider."[18] This type of policy risks not only creates conflicting standards and raises risk, but fundamentally undermines the security of these devices.[19]

Conflicting laws can also negatively impact innovation, especially for industries that rely on interstate networks. For example, a number of states have started to pass laws that require two-person crews on all freight trains, despite the fact that technology is evolving to allow one-person trains to operate as or even more safely and cost effectively.[20] As a result, a train going through one of the states with these rules would be required to come to a complete stop in order to add a superfluous conductor—an inefficient process, the costs of which will be borne by all U.S. train consumers.[21] Moreover, such steps will limit innovation in more autonomous rail operations.[22] Railways, like electricity transmission, natural gas pipelines, and telecommunications are inherently interstate and should be regulated where possible at the federal level. Similarly, states have started to create differing standards for the technology of connected and autonomous vehicles. While, traditionally, the U.S. Department of Transportation has focused on regulating how vehicles are built (e.g., setting airbag standards) and states have focused on regulating the operation of the vehicle (e.g., insurance, licensing, registration, traffic laws), these lines have started to blur—threatening to create a patchwork of differing standards for connected and automated vehicles operating across the United States. Since 2011, for example, 22 states have passed laws related to autonomous vehicles, some of which can act as barriers to these vehicles.[23]

States should tax what is being sold, not whether it is sold online or in brick-and-mortar stores.

Third, states have passed regulations that discriminate directly against digital products and services as well as telecommunications services. For example, states have passed discriminatory taxes on digital sales that are not placed on non-digital sales.[24] Ideally, states should tax products based on what is sold and not how it is sold. Most tax economists agree that digital goods and services should be taxed at the same rate as their physical counterparts.[25] Imposing higher taxes on digital goods—which are often consumed from out-of-state sellers—distorts the

market by encouraging consumers to purchase physical goods—which are often consumed from in-state sellers and normally have higher costs—instead of digital goods.

Fourth, many states create "middle-men" barriers to e-commerce, which prohibit certain digital activities to advantage incumbent intermediaries. One example is direct-to-consumer wine sales. Prior to a 2005 Supreme Court decision, state lawmakers often prohibited out-of-state wine sales to give competitive advantages to in-state wineries.[26] While the decision opened the door for winery and retailer direct-to-consumer wine-shipping, there is still a complicated state-based licensing system and several states still prohibit direct-to-consumer sales.[27] Similarly, states have banned direct-to-consumer sales of vehicles to maintain an advantage for car dealers in their state.[28] Moreover, states have a long history of passing anti-competitive laws that benefit optometrists by making it harder for customers to buy contact lens from other channels, including online sales.[29]

Finally, these policies often create spatial externalities in the sense that an individual state might capture the benefits from a discriminatory tax but the costs are imposed on the entire nation. We see that for example, in broadband and wireless taxes. All states and many localities have imposed taxes on wireless services in excess of regular sales tax rates.[30] But numerous academic studies have found that such taxes limit Internet adoption and use.[31] Because these are network technologies, the fewer number of subscribers resulting from these taxes imposes costs on the entire U.S. economy.

Case Studies

We present several major case studies where states have either failed to create a cohesive system or actively sought to create a segmented regulatory system, including in data privacy, taxes, net neutrality, money sending, and telehealth.

Data Privacy

Data privacy laws and regulations set the rules for how organizations collect, share, and reuse data. The United States has multiple federal and state laws that regulate data protection, often focusing on particular sectors or types of data, with multiple regulatory authorities responsible for oversight.[32] While U.S. federal law has created protections for some sectors of the economy (e.g., health care and financial services), states have also held a traditional role in enforcing privacy and property tort law, such as intrusion upon seclusion and public disclosure of private facts.[33] And while a number of comprehensive privacy bills have been proposed at the federal level, none have passed yet.[34]

Following the enactment of the General Data Protection Regulation (GDPR) in the European Union and the proposed introduction of California's privacy law, a growing chorus of voices is calling for federal privacy legislation.[35] While Congress has debated federal rules, states have acted. For example, in 2018 the California legislature rushed the California Consumer Privacy Act (CCPA)—which creates general privacy protections for all forms of data collection—into law to head off a more stringent proposal generated by referendum.[36] Similarly, the Washington state legislature tried to pass a separate and conflicting privacy law that ultimately failed.[37] New York also proposed privacy legislation for digital products and services that was more restrictive than California's, potentially creating mismatched rules between two of the United States' largest economies.[38] As of August 2019, at least 25 states and Puerto Rico have introduced bills related to data privacy.[39]

While only California has adopted a general data privacy law, states and localities have already enacted a myriad of privacy rules in specific industries and over specific types of data. For example, Illinois has created a privacy law for biometric data, such as fingerprints or facial scans.[40] The law was so strict that some companies have had to limit Illinoisans from using their mobile apps because they included facial recognition technology. Other states, such as Texas and Washington, have also passed biometric privacy laws.[41] Similarly, several states have considered and passed special measures regulating how Internet service providers can collect or share consumer data. In 2019, for example, 14 states introduced or considered broadband privacy laws, with Maine signing its proposal into law.[42]

Moreover, few existing federal privacy laws preempt states from creating additional rules. For example, many states have created privacy rules for health data that add to the regulations created by the Health Insurance Portability and Accountability Act of 1996, which already regulates the privacy and security protections for medical information controlled by certain entities.[43]

A national standard for consumer data privacy would eliminate the costs associated with 50 different state laws and avoid erecting artificial barriers across different parts of the Internet economy. As such, Congress should pass federal data privacy legislation that preempts state and local governments from passing their own laws that would go above or below a national standard or unfairly treat similar technologies differently.

Taxes

Since the creation of the Internet, Congress has addressed various taxes on online and digital activity. However, Congress has yet to address several major taxation issues: state taxes on wireless telecommunications, the collection of state sales taxes for online purchases, and the discriminatory state taxes on digital goods and services.

Wireless Telecommunications Taxes

In 1998, Congress recognized that unnecessary and excessive taxation could slow the growth of the Internet and reduce the benefits from the digital economy. To address this, Congress passed the Internet Tax Freedom Act (ITFA) to prohibit states from imposing taxes on Internet service and on incidental services, such instant messaging.[44] ITFA prohibits taxes on Internet service itself, whether the Internet Service Provider (ISP) is supplying dial-up, cable, digital subscriber line (DSL), fiber, or satellite. However, because wireless services did not yet exist in 1998, they fall outside of ITFA protections.

To date, all states and many localities have used this loophole to levy some form of tax on wireless service, with wireless consumers paying an estimated $16.1 billion in taxes, fees, and government surcharges to federal, state, and local governments in 2018.[45] These taxes affect consumption of wireless services, impacting purchasing decisions on things such as the number of minutes and services that consumers choose to buy.[46] Moreover, because wireless adoption is much more evenly distributed among income groups than fixed broadband, discriminatory taxes on wireless services have a disproportional impact on low-income households adopting these services—making these taxes more regressive than alternative forms of taxation.[47]

As ITIF has argued before, disproportionately high taxes on wireless services are an impediment to a stronger digital economy.[48] Therefore, Congress should seek to close this loophole in the existing prohibition on Internet services taxes.

E-commerce Taxes

States do have the power to require their residents to pay use taxes on sales, even when the seller is outside of their state borders and has no real connection with the state. This type of tax is not prohibited by the ITFA and was upheld in the 2018 Supreme Court decision *South Dakota v. Wayfair*.[49] Prior to *Wayfair*, companies had to have a physical nexus within a state in order to be responsible for paying sales taxes. As a result of this decision, each state and locality can set up its own rules on what can be taxed, the amount of those taxes, and more—creating an incredibly complex system where online retailers would need to be able to do hundreds of different tax calculations to sell their products across the United States.

Unfortunately, Congress and state governments have failed to streamline how states and localities tax remote sellers. States have been slow to adopt a common framework for taxing ecommerce sales. In 2002, several state governments came together to create the Streamlined Sales and Use Tax Agreement (SSUTA), an interstate agreement to simplify the process for registering with their tax agencies, with common definitions, rules, and simplified rate structures.[50] The goal of SSUTA was to reduce burdens on remote sellers. Unfortunately, SSUTA has been incredibly slow to deploy. As of September 29, only 24 states had signed onto the compact (with Tennessee achieving substantial but not full compliance with the effort).[51] Congress, for its part, has consistently introduced legislation to create a common system for state and local taxation of ecommerce since 2013.[52] It has also introduced a series of bills to turn back the *Wayfair* decision and once again create a physical nexus requirement (which would not address the underlying problem of mismatched regulations).[53] Each of these proposals have failed.

States clearly should have the authority to tax the sales of products purchased over the Internet (or by phone or mail), if for no other reason than as a matter of fairness. However, ecommerce requires that these tax systems impose the minimal compliance burden. As such, Congress should pass Internet sales tax legislation that allows states to tax out-of-state Internet sellers with or without a legal nexus if they abide by an easy-to-comply-with framework.

Taxes on Digital Goods and Services

Some states have created discriminatory taxes on digital goods and services, which are content that is downloaded over the Internet with no physical component, such as Netflix movies or iTunes music. Across the United States, states and local governments have created taxes that discriminate on the sale of digital goods and services, taxing them at different rates than their physical counterparts. There are 27 states that tax digital goods, with significant differences in definitions and what types of digital goods are taxed.[54] There are several types of taxable digital goods that may differ depending on the state: online data processing services, downloaded software, downloaded books, downloaded music, downloaded movies (or other digital video), and other downloaded goods. While states that are members of SSUTA use uniform definitions of these products, these definitions are not linked to the actual taxability of digital products, which varies from state to state.

Imposing higher taxes on digital goods can distort the market, pushing consumers to buy physical goods rather than digital options. Rather than giving an advantage to any particular distribution channel, congress should pass legislation prohibiting states from imposing discriminatory taxes on digital goods and services. Such legislation would recognize the importance of digital goods and services to the national economy and create a fair, consistent, and non-discriminatory tax system within which states can operate.

Net Neutrality

In 2018, the Federal Communication Commission (FCC) returned the legal classification of broadband access service from public utility legal classification back to the more lightly regulated information service.[55] The FCC decided Congress had not given it clear authority to act as the primary regulator of broadband, and functionally turned over this authority to the Federal Trade Commission (FTC). This abdication of authority had the effect of repealing the Obama-era net neutrality rules that were predicated on the new classification.

This light-touch approach—relying on the FTC to police broadband access providers through its ex-post enforcement of unfair or deceptive trade practices—left a perceived void that some states and localities were eager to fill. In 2018, 34 states and the District of Columbia introduced 120 bills and resolutions regarding net neutrality.[56] Five states, including California, New Jersey, Oregon, Vermont and Washington, enacted net neutrality legislation of one form or another. Some of these laws, such as that in Vermont, would prevent any broadband providers that do not abide by net neutrality rules from receiving contracts to provide service for state government users.[57] Others go further. For example, the California Internet Consumer Protection and Net Neutrality Act of 2018 prohibits fixed and mobile Internet service providers (ISPs)—which provide broadband Internet service—from engaging in specified actions, such as blocking or slowing lawful Internet traffic.[58] California and Vermont face lawsuits from the Department of Justice and the broadband industry. Both states reached agreements to hold off on enforcing the laws, pending a decision in the primary challenge to the FCC's *Restoring Internet Freedom Order*.[59] In October of 2019, the U.S. Court of Appeals for the D.C. Circuit made clear that the FCC does not have the legal authority to make a blanket preemption of state-level net neutrality laws.[60] Instead, the analysis of to what extent various state net neutrality laws conflict with federal policy will have to be done on a case-by-case basis, all but guaranteeing continued confusion and conflict between state and federal policies here.[61]

State actions have generated a great amount of uncertainty for national and regional networks, which should be subject to uniform rules to keep compliance costs low and reduce complexity.[62] Broadband networks are designed to cover large regions, and it could be practically difficult to implement multiple conflicting state laws. The original technological justifications for local- or state-level control over telecommunications are quickly eroding: Communications have become largely distance-insensitive, applications and network functions are separate from the central offices located within a state, and broadband transmissions rarely stay within a single state's borders.[63] When it comes to prioritization, the technology that ISPs use to differentiate data traffic, the real value would be to latency-sensitive applications, such as teleconferencing. Because distance adds unavoidable latency, prioritization would be most beneficial for interstate communications, meaning that in an ideal world, federal legislators would craft a carefully balanced policy at the federal level.

Unfortunately, as stated above, the transfer of broadband oversight to the Federal Trade Commission created a perceived void that state legislators looked to fill with efforts to regulate net neutrality. Regardless of the specific substantive rules, it is incumbent on federal policymakers to step in and create national net neutrality legislation that restores FCC authority and preempts state actions.[64]

Money Sending Laws

Local regulation for the financial services industry made sense when local brick-and-mortar banks handled payments, insurance, loans, and consumer finances. Even when money was transferred across borders—both before and after banks started adopting information technology—this system of banks was often necessary to handle the processing and security of payments and transfers, creating an expensive, time-consuming, and intermediary-driven system.[65] This system also necessitated regulators in each jurisdiction to hold local financial services companies accountable for their fiduciary responsibilities.

The Internet and mobile technology have changed how people transmit money, enabling faster, cheaper, and more convenient payment and transfer systems that do not require local banks. However, while the payment landscape has changed, the regulatory environment remains largely intact. To send payments to recipients in other states, payment companies need to acquire state-issued money sender or transmitter licenses from each state. There are currently 53 states and territories that have individual licensing requirements for money transmitters.[66] These laws and certifications conflict between different states, and businesses that try to break out in the payment space are saddled with getting complicated and expensive licenses for each state in which they operate. Given that each of these licenses can cost over $1 million each and that it can take two years for the application to get approved, this burden is often simply too much for some businesses offering innovative solutions.[67] These costs come from minimum holdings, bond fees, application fees, audit fees, anti-money laundering costs, and more.

Fortunately, some states have made progress towards harmonizing their money transmitter rules. Several states—Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas, and Washington (collectively, "Signatory States")—have taken steps to standardize licensing practices for payment systems.[68] Moreover, the U.S. Office of the Comptroller of the Currency (OCC) has attempted to create a charter for certain financial companies, allowing them to send money, and offer deposit and loan services without complying with state regulations.[69] This charter, which has been the subject of litigation from various states, would enable some companies to avoid complying with conflicting sets of state rules when sending money.[70] Federal regulators, such as the OCC, should continue to explore ways for national payment companies to avoid complex and conflicting state money sending regulations. However, this style of program only helps a limited number of payment companies that can apply for the program. Congress should create a national framework for money sending laws that harmonizes state rules, especially definitions, and further empowers federal regulators to remove state and local barriers to payment technologies, such as cryptocurrencies.[71]

Telehealth

Telehealth applications enable medical providers to diagnose and treat patients remotely.[72] With telemedicine solutions, patients in rural areas who do not have easy access to life specialists due to a lack of local expertise and high travel costs can still receive medical consultations. One

2017 study of 20,000 patients found they could save millions of dollars of direct travel costs due to telehealth solutions.[73] Urban populations also stand to benefit from lower cost and greater access. For example, one 2018 study showed telehealth solutions deployed in Rochester, New York, vastly improved patient outcomes for children with asthma.[74]

The promise of this technology, unfortunately, has been negatively impacted by state licensing and certification laws. Because states have traditionally overseen the licensing of physicians, to offer U.S.-wide services, clinicians must apply for a license in each state they want to serve, which would require dozens of licenses, payments of thousands of dollars in application and licensing fees to each state's medical board, and burdensome efforts to comply with myriad changing state rules.[75] This structure makes it very difficult for out-of-state doctors to offer remote care. Moreover, because patients in this system are often forced to choose doctors licensed to practice in their state, state licensing shields doctors from competition.

States have started to create a more harmonized system. The Federation of State Medical Boards established an Interstate Medical Licensure Compact, which allows physicians licensed in any state belonging to the compact to practice in all states.[76] Currently, 29 states, the District of Columbia and the Territory of Guam all participate.[77] However, as one author wrote, "the compact protects the power of state medical boards to shield physicians in their states from competition. It [also] preserves the multiple fees physicians must pay to each state board."[78] Federal intervention may be necessary to ensure states do not continue to increase costs and stifle interstate competition in telemedicine.[79] Indeed, in 2018 the U.S. Department of Veterans Affairs (VA) passed a rule that preempts state laws and allows VA healthcare providers to deliver care through telehealth to VA beneficiaries across state lines.[80] Lawmakers in Congress should introduce legislation to circumvent the state licensing requirements and establish a single, national license for telehealth providers. The TELE-MED Act, which was introduced in the 113th and 114th Congress, would have allowed Medicare providers licensed in one state to provide services to Medicare beneficiaries in another.[81] Congress should again take up this issue.

THE CASE FOR A U.S. DIGITAL SINGLE MARKET

The federal and state governments will need to take specific steps to develop a digital single market for the United States. Inaction, or limited action, will relegate the United States to having a fragmented market for digital goods and services, at a time when China and the European Union are moving in the other direction.

There have certainly been cases of success where Congress has acted to preempt state and local laws These include rules for certain Internet taxes, giving consumers rights to obtain contact lens prescriptions, recognizing digital signatures, prohibiting non-disparagement clauses in consumer sales, and regulating wireless Internet services. These are all useful examples of how a U.S. digital single market offers many potential benefits.

First, creating a national standard guarantees the same protections for all U.S. residents, ensuring that consumers in states that fail to enact consumer protection regulation are protected by federal laws. Take, for example, consumer reviews, which are a vital and important part of the digital economy, enabling users to share their good and bad experiences about the goods and services they use. But until 2016, it was legal in several states for businesses to deploy contract provisions that inhibited their consumers from negatively reviewing them.[82] To remedy this and

create a standard across the United States, Congress passed the Consumer Review Fairness Act in 2016, which voided certain anti-reviewer contract provisions.[83] Similarly, when Congress passed the Fairness to Contact Lens in 2003, the goal was to charge the Federal Trade Commission with setting national rules to give lens consumers the right to their prescription.[84] Congress should take similar measures to create national protections for other consumer protection issues, like data privacy protections, data breach notifications, net neutrality, and strategic lawsuits against public participation (SLAPPs), and ensure that these preempt state laws.[85]

Second, national rules minimize transaction costs for businesses, the benefits of which are passed along to users. Without federal preemption, businesses must apply for and receive licensing, or simply comply with differing regulations in each state that they operate. For example, if Maine and California require different standards for data privacy rules (e.g., obtaining consent or providing data portability), an organization operating in both would be subject to the higher costs of implementing dueling compliance regimes than if the two states had identical privacy regimes.[86] Indeed, differing state licensing regimes increase costs significantly. National rules also reduce transaction costs related to uncertainty and confusion over how rules affect novel technology applications for businesses operating in multiple states. For example, prior to state and federal action that created legal certainty for digital signature in the United States, online transactions existed in a legal grey area.[87] This uncertainty and accompanying legal risk unnecessarily raised costs for businesses wanting to engage in online commerce.

The costs that arise from state and local enforcement are largely unnecessary and redundant as technology has rendered location of where a service is offered less important. For example, in telecommunications networks, the cost of transit in packet-routed networks is largely distance-insensitive, meaning there is no technological reason communications over state boundaries must cost more or be treated differently than communications that remain within one state's borders. Networks and services are also now modular, with applications largely separated from the underlying network. And many of the network functionalities are being virtualized or shifted the edge of the network entirely, further reducing the importance of location-specific regulation.[88]

Third, a U.S. digital single market will encourage economies of scale, whereby the per-user cost to a firm of providing services tends to fall with each additional customer. For example, in wireless broadband, harmonized regulations drive gains throughout the entire mobile value chain by enabling cheaper per-unit infrastructure cost, a more uniform radio environment, greater interoperability and scale for end-user devices, and a larger platform for digital services.[89] Similarly, Internet services that operate on low overhead often rely on economies of scale to offer free or low-cost services.[90] Economies of scale also produce better network effects that are more beneficial to more users. The classic example is telephone service, which becomes more valuable to a user if more people are connected. Indeed, telephone network externalities have long been recognized and have been a major rationale behind universal service policies. For example, broadband has network effects in part because the decision to purchase broadband is dependent to a degree on having sufficient knowledge about its benefits. Unlike a service like haircuts or a product like TVs that most people are familiar with and can accurately ascertain the value of, fewer people are familiar with wireless data and Internet services and cannot always put a value

on their benefits. Indeed, research suggests that people are more likely to adopt telecom services if they live in an area with high adoption levels.[91]

Fifth, a digital single market will increase efficiency in the policymaking process. When 50 different states make laws on the same topics, stakeholders must engage in the same policy debates in multiple forums. This creates an enormous amount of waste and leads to less-than-optimal outcomes, especially for less well-funded stakeholders who may not have the resources to participate in every state.

Finally, a U.S. digital single market will reduce negative externalities caused by state and local actions. Understandably, local communities sometimes put their narrow interests ahead of national goals. This often takes the form of imposing fees that are ultimately passed on to those outside their jurisdiction or accommodating populist backlash to perceived threats.

Here 5G deployment efforts provide good examples.[92] Some communities have cited unfounded claims around the health effects of wireless signals to challenge cell tower deployments.[93] Radio emissions used for wireless broadband are significantly below the frequencies that can knock electrons from an atom—so-called ionizing radiation—and are thus much safer than sunlight, for example. National guidelines already set safety limits around the appropriate power levels for different types of transmissions, however, more could be done to ensure every city council and state legislature does not have to debate this topic before granting approvals or denials to put up telecommunications towers. Moreover, some localities—usually those with relatively wealthy, high-demand broadband customers—have sought to impose high and discriminatory fees on the deployment of wireless infrastructure. These cities know they receive revenue from carriers, the costs of which are spread over the companies' entire customer base. If they set these fees at the maximum rate at which operators will still deploy, they enjoy a respectable source of cash (without raising taxes) paid for by wireless customers outside their jurisdiction, while still getting high quality 5G deployments.[94] Cities have important legitimate interests when it comes to how infrastructure is deployed in their jurisdictions, but a uniform process should encourage a more rapid deployment of 5G and reduce the potential externality imposed by those relatively few cities looking to line the city coffers with money that might otherwise go toward broadband deployment.

Lessons from Europe's Digital Single Market

There are many lessons that U.S. policymakers can take from Europe's attempts to create a cohesive set of rules for its digital economy. In May 2015, the Europe Union passed a law to create a Digital Single Market (DSM) to incorporate the digital economy into European integration.[95] In many respects, European DSM has been a success. For example, the European Union created the Single Euro Payments Area (SEPA) that simplified payments throughout the entire economic area.[96] In addition, Europe has attempted to harmonize how it responds to cyber-attacks and has attempted to modernize its copyright rules across the entire region.[97] Indeed, Europe has created a single standard for data breach notification.[98]

Some of these efforts, however, have resulted in negative impacts for both Europe and the globe. In pursuit of the DSM, Europe created the GDPR to establish EU-wide rules on data protection. On one hand, these rules created certainty and uniformity making it easier for digital firms to do business throughout the European Union. On the other hand, these rules hurt the global digital market and European innovation. For one, GDPR imposes restrictions on European data traveling outside its borders with an untenable and impractical approach that limits global data flows.[99] In addition, GDPR also imposed new, unnecessary and futile restrictions on emerging technology. For example, GDPR imposed rules that could limit the use and development of artificial intelligence, such as the so-called "right to explanation," which limits organizations from using some types of deep learning which may be more accurate but less explainable.[100]

U.S. policymakers should avoid Europe's mistakes by establishing the U.S. digital single market while avoiding unnecessarily stringent rules that limit innovation and discourage global commerce.[101]

HOW TO CREATE A U.S. DIGITAL SINGLE MARKET

Companies in the United States will be most successful if they have access to larger markets with one uniform set of regulations. When state and local governments create multiple and often conflicting laws and regulations, it raises compliance costs, reduces national growth and competitiveness, and limits consumer choice.

A national U.S. marketplace for digital products and services is necessary to maximize interstate digital commerce. Usually this will require Congressional action to preempt state and local action in favor of a unified national framework. However, in other cases states can work in tandem to create interstate regulatory alignment.

None of this is to imply that federalism should not remain a bedrock principle of U.S. governance. States and local governments should continue to innovate in a wide array of areas, including digital issues, that do not affect interstate commerce. For example, states should pursue a variety of policies that increase wireless and broadband services adoption. This type of experimentation is important, not only because some solutions that work in one place may not work in other places, but also because of the "laboratories of democracy" effects where policy innovations in one state flow to others, or even the federal level. But in policy areas that are inherently interstate—and that involves most digital regulatory issues today—Congress will have to play the lead role in protecting and enabling a U.S. digital single market by working with states to facilitate interstate dialogue or creating the national rules when states disagree on

national legislative outcomes. This so-called "cooperative federalism" is not always an easy process, as states and the federal government constantly fight over the balance of power in the context of Internet and telecommunications policy, but ensuring uniformity and consistency will maximize the potential of the U.S. digital economy.

There are several steps that both federal and state policymakers can take to achieve this goal.

First, states should enter into multi-state compacts that create national legal standards where they have common goals. A good example of this type of action occurred when states look the lead in ensuring the legal certainty of e-signatures. In the late-1990s and early 2000s, users were rapidly starting to use the Internet for commerce. But while U.S. laws gave legal legitimacy to "wet" signatures, they did not do the same for digital ones. To remedy this, U.S. states adopted the Uniform Electronic Transactions Act (UETA) in 1999, which set requirements for electronic signatures to be valid.[102] However, only 47 states adopted UETA. To create a national framework in the United States, in 2000, Congress passed the Electronic Signatures in Global and National Commerce Act, which effectively preempts states from creating additional e-signature laws unless they follow UETA.[103] States are also pursuing the path, although to a lesser degree of success, with money-sending licenses, cross-state medical licensing, and more. Certainly, not all states will agree to these interstate compacts. The federal government should bolster these efforts by setting a federal backstop for states that do not sign onto multistate efforts—ensuring users across the United States receive the same protections and businesses know the rules of the road for operating anywhere in the United States.

Second, states should create reciprocity agreements when they cannot agree on the same rules. For example, in telehealth, states may not decide to agree on the same rules for the qualifications to be a licensed doctor, but they should agree that a doctor qualified to provide telehealth services in North Dakota can provide telehealth services in South Dakota.

Third, when states cannot agree on a common path forward, or establish reciprocal agreements; or in areas where it is simply easier to create a top-down national framework, such as privacy regulation, Congress should pass federal legislation on major digital issues that preempts states from creating conflicting rules. The goal of federal legislation should also be to streamline regulations by creating a single, national standard, rather than simply adding another layer of regulatory complexity. Therefore, federal legislation should set both a floor and a ceiling so that states cannot create more-stringent rules than the standard.

For issues such as privacy, security, taxes and net neutrality, Congress either has already drafted a national solution or is actively working on the problem. Sen. John Thune (R-SD) reintroduced the Digital Goods and Services Tax Fairness Act in 2019 to prohibit discriminatory digital taxes and stop states from imposing multiple taxes on the sale of electronic goods.[104] Similarly, Reps. Josh Gottheimer (D-NJ) and 47 other Democrats have sought to convene a bipartisan working group to create federal legislation for net neutrality.[105] Another Congressional proposal, called the Ensuring National Constitutional Rights for Your Private Telecommunications (ENCRYPT) Act, which was last introduced by Rep. Ted Lieu (D-CA) in 2018, would prohibit states from requiring companies to weaken encryption or deploy backdoors for law enforcement.[106] And several senators are currently drafting federal privacy legislation that could preempt multiple and duplicative state actions.[107]

Importantly, preemption does not mean states should sit out of the process. Rather than reducing state enforcement power, legislative efforts should expand it. For example, the Dodd-Frank Act authorized state attorneys general to bring civil action against companies that engaged in unfair, deceptive or abusive practices.[108] Federal rules should ensure state attorneys' general can help enforce privacy, data breach, net neutrality, or other federal rules. When enabling state attorneys general to pursue enforcement actions under a federal law, Congress should protect against duplicative or inconsistent enforcement. It can do so by empowering federal regulators to take over cases where there is shared jurisdiction to ensure consistent enforcement.

Finally, the Federal Trade Commission (FTC) or other relevant federal regulators should do more to identify and challenge state and local barriers to a U.S. digital single market. As part of their review of federal enforcement, regulators should review the actions of state and local policymakers to regulate the digital economy and identify practices that create anticompetitive barriers. Sometimes anti-competitive policies are the result of well-meaning restrictions that have the unintended consequence of creating anticompetitive barriers. For example, some incumbent taxicab companies have convinced local taxi commissions to create rules benefiting them at the expense of new entrants to the market. State and local officials may be reluctant to remove anticompetitive policies in the face of resistance from incumbents, even if they result in worse outcomes for consumers. Regulators should look to examples such as anti-competitive barriers in optometry, real estate, and direct-to-consumer sale of vehicles to better understand this challenge.

Once identified, federal regulators should use every tool at their disposal to create rules to unify digital regulations across the United States. Regulators can generally do this in one of three ways. First, if their statutes allow it, they can write rules that directly preempt states. For example, through the Telecom Act of 1996, the FCC can create net neutrality rules in a way that preempts certain conflicting price regulations by states and localities.[109] Second, federal regulators should create regulatory systems for companies to circumvent existing legal quagmires.[110] For example, the Office of the Comptroller of the Currency created a fintech charter to enable certain licensed businesses to circumvent the myriad state money-sending and banking laws and only deal with one regulator.[111] Finally, regulators should preempt state and local rules before they are implemented in anti-competitive or harmful ways. As former FTC Commissioner Joshua Wright has argued, "the FTC is in a good position to use its full arsenal of tools to ensure that state and local regulators do not thwart new entrants from using technology to disrupt existing marketplaces."[112] Indeed, in a 2015 Supreme Court decision, the Court reiterated that federal antitrust laws that safeguard against anticompetitive practices apply to state and local actions.[113] And, where needed, Congress should pass legislation preempting protectionist state rules, as they did with the Fairness to Contact Lens Consumers act.[114]

CONCLUSION

The United States still lacks a digital single market in large part because state and local governments continue to pass conflicting laws and Congress does not always act to preempt those laws. The lack of an integrated national market holds back innovation and limits consumer welfare.

In theory, it should not matter whether states or Congress sets the rules, as long as the outcome is a consistent national framework. The challenge is that states are more willing to intervene with

inconsistent rules, whereas Congress is more likely to create consistent rules, but less likely to intervene. In Congress, all too often Republicans are hesitant to regulate the digital economy, in part because of well-justified concerns about harming innovation. And all too often Democrats are more willing to regulate, but worry that Washington will not pass legislation with adequate strength and therefore want activist states to be able to raise the bar. While both views are understandable, the result is all too often stalemate, with states as the default setter of U.S. digital economy policy. Indeed, one reason why some states have intervened is because the federal government has too often not acted, and this reluctance opens up space for state governments with fewer concerns to step in.

It is time for that to change. Congress needs to understand that a digital economy places many more economic regulatory issues in its hands and that it needs to act to ensure adequate regulatory protection but in ways that create one, and only one, governance framework for the entire U.S. economy. If states become more proactive in developing multi-state compacts or demonstrate an ability to craft uniform national laws, then Congress can take a step back from this role. But if states continue to pursue their own individual and conflicting laws, the current views in Washington with regard to preemption on digital policy issues need to change and be replaced with agreement that national rules should be the priority.

About the Authors

Alan McQuinn is a senior policy analyst at the Information Technology and Innovation Foundation. He writes and speaks on a variety of issues related to information technology and Internet policy, such as cybersecurity, privacy, blockchain, fintech, e-government, Internet governance, intellectual property, and aerospace. He was previously a telecommunications fellow for Representative Anna Eshoo (D-CA). McQuinn graduated from the University of Texas at Austin with a B.S. in public relations and political communications and a minor in Mandarin Chinese.

Daniel Castro is vice president of ITIF and director of ITIF's Center for Data Innovation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office, where he audited IT security and management controls at various government agencies. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.

ENDNOTES

1. U.S. Const. Article I. Section 8. Clause 3.
2. Ira Magaziner, "Creating a Framework for Global Electronic Commerce" (Progress & Freedom Foundation, July 1999) http://www.pff.org/issues-pubs/futureinsights/fi6.1globaleconomiccommerce.html.
3. Communications Decency Act, 47 U.S.C. §230 (1996); Internet Taxation Freedom Act, P.L. 105-277 (1998).
4. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 96 (2000).
5. Dana Nigro, "U.S. Supreme Court Overturns Wine-Shipping Bans," *Wine Spectator*, May 2005, https://www.winespectator.com/articles/us-supreme-court-overturns-wine-shipping-bans-2543.
6. James H. Johnston and Robert D. Atkinson, "Power of Attorneys: Will the Organized Bar Thwart the Emergence of Online Law?" (Information Technology and Innovation Foundation, July 2006), https://itif.org/publications/2006/07/10/power-attorneys-will-organized-bar-thwart-emergence-online-law. For example, see this report on online legal services.
7. California Civil Code § 1798.100 - § 1798.198 (2018). For example, in 2018, California enacted a sweeping data privacy law.
8. New State Ice Co. v. Liebmann, 285 S. Ct. 262 (1932).
9. Nigel Cory and Stephen Ezell, "Comments to the U.S. International Trade Commission Regarding the United States-Mexico-Canada Agreement" (Information Technology and Innovation Foundation, September 2019).
10. "Shaping the Digital Single Market, "European Commission, July 4, 2019, accessed September 19, 2019, https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.
11. Robert D. Atkinson and Stephen Ezell, "Promoting European Growth, Productivity, and Competitiveness by Taking Advantage of the Next Digital Technology Wave" (Information Technology and Innovation Foundation, March 2019), http://www2.itif.org/2019-europe-digital-age-a4.pdf.
12. California Civil Code § 1798.100 - § 1798.198 (2018).
13. Robert D. Atkinson, "The 2014 ITIF Luddite Awards," (Information Technology and Innovation Foundation, January 2015), http://www2.itif.org/2015-luddite-awards.pdf.
14. Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use" (Information Technology and Innovation Foundation, July 2018), http://www2.itif.org/2018-trust-privacy.pdf.
15. Alan McQuinn and Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law" (Information Technology and Innovation Foundation, August 5, 2018), https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.
16. U.S. Const. Article I. Section 8. Clause 3.
17. Chris Cwalina et al., "Nine States Pass New and Expanded Data Breach Notification Laws," (Norton Rose Fulbright, June 2019), accessed September 16, 2019, https://www.dataprotectionreport.com/2019/06/nine-states-pass-new-and-expanded-data-breach-notification-laws/.
18. A.B. 1681, California Civil Code § 22762 (2016).
19. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (Information Technology and Innovation Foundation, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.

20. Justin Franz, "Colorado becomes fifth state to require two-person crews in Locomotive Cabs" *Trains*, March 22, 2019, accessed September 16, 2019, http://trn.trains.com/news/news-wire/2019/03/22-colorado-becomes-fifth-state-to-require-two-person-crews-in-locomotive-cabs.
21. Nick Zaiac, "Barriers to Innovation and Automation in Railway Regulation" (R Street, June 2019), accessed September 16, 2019, https://www.rstreet.org/2019/06/24/barriers-to-innovation-and-automation-in-railway-regulation/.
22. Joe Kennedy, "The Federal Railroad Administration Makes the Right Call on Railroad Staffing Requirements," (Information Technology and Innovation Foundation, May 2019), https://itif.org/publications/2019/05/30/federal-railroad-administration-makes-right-call-railroad-staffing.
23. "Autonomous Vehicles | Self-Driving Vehicles Enacted Legislation," National Conference of State Legislatures, September 18, 2019, accessed September 19, 2019, http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx.
24. Scott Andes and Robert D. Atkinson, "A Policymaker's Guide to Internet Tax" (Information Technology and Innovation Foundation, March 2013), http://www2.itif.org/2013-policymakers-guide-internet-tax.pdf.
25. Robert D. Atkinson, "Wireless Taxation, Economic Growth and Economic Opportunity," (Information Technology and Innovation Foundation, 2009), Before the Committee on the Judiciary and Subcommittee on Commercial and Administrative Law, http://www.itif.org/files/Wireless_testimony.pdf.
26. Nigro, "U.S. Supreme Court Overturns Wine-Shipping Bans," Granholm v. Heald, 544 S. Ct. 460 (2005).
27. "Direct-To-Consumer Shipping Laws for Wineries," *Wine Institute*, 2019, accessed September 19, 2019, https://wineinstitute.compliancerules.org/state-map/.
28. Atkinson, "The 2014 ITIF Luddite Awards."
29. Robert D. Atkinson, "Why UPP Pricing in the Contact Lens Industry Hurts Consumers and Competitions" (Information Technology and Innovation Foundation, July 2014), comments to the U.S. Senate Committee on Judiciary, http://www2.itif.org/2014-senate-contact-lens.pdf.
30. Scott Mackey and Joseph Bishop-Henchman, "Wireless Taxes and Fees Climb Again in 2018," (Tax Foundation, December 2018), accessed September 19, 2019, https://files.taxfoundation.org/20181210141036/Wireless-Taxes-and-Fees-Climb-Again-in-2018-FF-626-2.pdf.
31. Scott Andes and Robert D. Atkinson, "A Policymaker's Guide to Internet Tax" (Information Technology and Innovation Foundation, March 2013), http://www2.itif.org/2013-policymakers-guide-internet-tax.pdf.
32. Nick Wallace et al., "How Canada, the EU, and the U.S. Can Work Together to Promote ICT Development and Use" (Information Technology and Innovation Foundation, June 2018), http://www2.itif.org/2018-canada-eu-us-ict-development.pdf.
33. William Prosser, "Privacy," California Law Review 48, (1960), 3, accessed September 24, 2019, http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview.
34. Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America" (Information Technology and Innovation Foundation, January 2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf.
35. Ibid.

36. Marc Vartabedian, "California Passes Sweeping Data-Privacy Bill," *Wall Street Journal*, June 28, 2018, accessed September 16, 2019, https://www.wsj.com/articles/california-rushe.s-to-tighten-data-privacy-restrictions-1530190800.
37. Lucas Ropek, "Why Did Washington State's Privacy Legislation Collapse?" *Govtech*, April 19, 2019, https://www.govtech.com/policy/Why-Did-Washington-States-Privacy-Legislation-Collapse.html.
38. An Act to Amend the General Business Law, in Relation to the Management and Oversight of Personal Data, New York SB 5642 (2019).
39. "2019 State Legislation Related to Consumer Data Privacy," National Conference of State Legislatures, August 13, 2019, accessed September 16, 2019, http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.
40. Biometric Info. Privacy Act, § 740 ILCS 14 (2008).
41. "Washington Becomes the Third State with a Biometric Law," *Inside Privacy*, May 31, 2017, accessed September 16, 2018, https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-statewith-a-biometric-law/.
42. "2019 State Legislation Related to Consumer Data Privacy," National Conference of State Legislatures.
43. The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936, (1996).
44. Internet Taxation Freedom Act, P.L. 105-277 (1998).
45. Mackey and Bishop-Henchman, "Wireless Taxes and Fees Climb Again in 2018."
46. Andes and Atkinson, "A Policymaker's Guide to Internet Tax."
47. Ibid.
48. Ibid.
49. South Dakota v. Wayfair, Inc., 138 S. Ct. 2080 (2018).
50. "State Information" Streamlined Sales Tax Governing Board, Inc., 2018, accessed September 16, 2019, https://www.streamlinedsalestax.org/Shared-Pages/State-Detail.
51. Ibid.
52. Market Place Fairness Act, S. 698 (2015), 114th Cong. (2015).
53. Protecting Businesses from Burdensome Compliance Cost Act of 2018, H.R.6724 (2018), 115th Cong. (2018). This is one of several examples.
54. Victoria Venn, "Sales Tax for Digital Products in the U.S.," Quaderno, September 10, 2019, accessed September 19, 2019, https://quaderno.io/blog/sales-tax-digital-products-us/.
55. Restoring Internet Freedom, WC Docket No. 17-108. Report and Order, Declaratory Ruling, and Order, 33 FCC Rcd 311 (1) (2018).
56. "Net Neutrality Legislation in States," National Conference of State Legislatures, January 23, 2019, accessed September 16, 2019, http://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-legislation-in-states.aspx.
57. Act 169, Chapter 22, 2 VSA § 754 (2018).
58. California Internet Consumer Protection and Net Neutrality Act of 2018, California Civil Code § 5096 - § 17914 (2018).
59. Brian Fung, "California Agrees Not to Enforce its Net Neutrality Law as Justice Department Puts Lawsuit on Hold," *Washington Post*, October 26, 2018, accessed September 26, 2019, https://www.washingtonpost.com/technology/2018/10/26/california-agrees-not-enforce-its-net-neutrality-law-trumps-doj-puts-its-lawsuit-hold/.

60. Mozilla v. FCC (D.C. Cir. 2019) available at https://www.cadc.uscourts.gov/internet/opinions.nsf/FA43C305E2B9A35485258486004F6D0F/$file/18-1051-1808766.pdf.

61. Ibid at 121 to 145. Note the court only vacated the FCC's preemption insofar as it was categorical, but explicitly makes clear that individual state laws that are in conflict with the federal policy can be struck down under conflict preemption or other legal theories.

62. Doug Brake, "National Networks Need National Policies," (Information Technology and Innovation Foundation, Nov. 2017), https://itif.org/publications/2017/11/09/national-networks-need-national-policies.

63. Douglas C. Sicker, "The End of Federalism in Telecommunication Regulations?" Northwester Journal of Technology and Intellectual Property, Issue 2 Volume 3 at 130 (2005), *available at* https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1032&context=njtip.

64. Doug Brake, "Why We Need Net Neutrality Legislation, and What It Should Look Like" (Information Technology and Innovation Foundation, May 2018), http://www2.itif.org/2018-net-neutrality-legislation.pdf.

65. Alan McQuinn, Weining Guo, and Daniel Castro, "Policy Principles for Fintech" (Information Technology and Innovation Foundation, October 2016), http://www2.itif.org/2016-policy-principles-fintech.pdf.

66. Ashley Grimes, "Money Transmitter Licensing" Grimes Law PLLC, accessed September 16, 2019, http://www.grimeslawaz.com/money-transmitter-licensing/; Thomas Brown, "50-State Survey: Money Transmitter Licensing Requirements," UC Berkeley Law School and Partner, Paul Hastings LLP, accessed September 16, 2019, https://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/50%20State%20Survey%20-%20MTL%20Licensing%20Requirements(72986803_4).pdf.

67. "Money Transmitter License Cost" *Faisalkhan*, accessed September 16, 2019, https://faisalkhan.com/services/money-transfer-license-money-transmitter-license/us-money-transmitter-license/money-transmitter-license-cost/.

68. "State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments," *CSBS*, February 6, 2018, accessed September 16, 2019, https://www.csbs.org/state-regulators-take-first-step-standardize-licensing-practices-fintech-payments.

69. U.S. Office of the Comptroller of the Currency, "OCC Begins Accepting National Bank Charter Applications From Financial Technology Companies," press release, 2018, accessed September 16, 2019, https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-74.html.

70. Alan Kaplinsky, "State Regulators File Second Lawsuit Opposing OCC Fintech Charter," Ballard Spahr LLP, October 29, 2018, accessed September 16, 2019, https://www.consumerfinancemonitor.com/2018/10/29/state-regulators-file-second-lawsuit-opposing-occ-fintech-charter/.

71. Alan McQuinn and Daniel Castro, "A Policymaker's Guide to Blockchain" (Information Technology and Innovation Foundation, April 2019), https://itif.org/publications/2019/04/30/policymakers-guide-blockchain.

72. Daniel Castro, Ben Miller, and Adams Nager, "Unlocking the Potential of Physician-to-Patient Telehealth Services" (Information Technology and Innovation Foundation, May 2014), http://www2.itif.org/2014-unlocking-potential-physician-patient-telehealth.pdf.

73. Navjit Dullet et al., "Impact of a University-Based Outpatient Telemedicine Program on Time Savings, Travel Costs, and Environmental Pollutants" Value in Health, April 2017, Volume 20, Issue 4, Pages 542–546, https://www.valueinhealthjournal.com/article/S1098-3015(17)30083-9/fulltext.

74. Jill Halterman et al, "Effect of the School-Based Telemedicine Enhanced Asthma Management (SB-TEAM) Program on Asthma Morbidity," JAMA Network, March 5, 2018, 172(3), https://jamanetwork.com/journals/jamapediatrics/article-abstract/2667559?redirect=true.
75. Shirley Svorny, "Telemedicine Runs Into Crony Doctoring," *Wall Street Journal*, July 22, 2016, accessed September 19, 2019, https://www.wsj.com/articles/telemedicine-runs-into-crony-doctoring-1469226979.
76. "The IMLC," *Interstate Medical Licensing Compact,* accessed September 19, 2019, https://imlcc.org/.
77. Ibid.
78. Svorny, "Telemedicine Runs Into Crony Doctoring."
79. Ibid.
80. Department of Veteran's Affairs, "Authority of Health Care Providers To Practice Telehealth," published in the Federal Register, May 11, 2018, accessed September 19, 2019, https://www.federalregister.gov/documents/2018/05/11/2018-10114/authority-of-health-care-providers-to-practice-telehealth.
81. TELE-MED Act of 2015, H.R.6724 (2015), 114th Cong. (2015).
82. Eric Goldman, "Understanding the Consumer Review Fairness Act of 2016," Michigan Telecommunications and Technology Law Review, Vol. 24, Iss. 1, 2016, accessed September 16, 2019, http://www.mttlr.org/wp-content/journal/voltwentyfour/goldman.pdf.
83. The Consumer Review Fairness Act of 2016, Pub.L. 114–258.
84. Fairness to Contact Lens Consumers Act, Pub.L. 108–164.
85. Daniel Castro and Laura Drees, "Why We Need Federal Legislation To Protect Public Speech Online" (Information Technology and Innovation Foundation, May 2015), http://www2.itif.org/2015-anti-slapp.pdf.
86. McQuinn and Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law."
87. "UETA and ESIGN Act," DocuSign, accessed September 16, 2019, https://www.docusign.com/learn/us-electronic-signature-laws-and-history.
88. *See* Sicker *supra*.
89. Doug Brake, "Spectrum Policy and the EU Digital Single Market: Lessons from the United States" (Information Technology and Innovation Foundation, December 2015), http://www2.itif.org/2015-eu-spectrum-policy.pdf.
90. Alan McQuinn, "No, Users are not Paying with their Data," *Inside Sources*, August 7, 2018, https://www.insidesources.com/no-internet-users-not-paying-data/.
91. Austan Goolsbee, "The Value of Broadband and the Deadweight Loss of Taxing New Technology," Contributions to Economic Analysis & Policy 5, no.1 (2006), www.bepress.com/bejeap/contributions/vol5/iss1/art8.
92. Doug Brake, "Comments of ITIF in the Matter of Accelerating Wireline and Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment" WC Docket No. 17-84, WT Docket No. 17-79 (June 2017), https://itif.org/publications/2017/06/15/comments-federal-communications-commission-spurring-broadband-deployment.
93. Danny Crichton, "Bay Area City Blocks 5G Deployments Over Cancer Concerns," *TechCrunch*, September 10, 2018, accessed September 10, 2019, https://techcrunch.com/2018/09/10/bay-area-city-blocks-5g-deployments-over-cancer-concerns/.
94. Doug Brake, "Standing in the Way of Next-Gen Wireless: What Gives, Mayor Liccardo?" *Information Technology and Innovation Foundation,* November 2017, accessed September 19, 2019, https://itif.org/publications/2017/11/06/standing-way-next-gen-wireless-what-gives-mayor-liccardo.

95. European Commission, "Digital Single Market: Commission calls for swift adoption of key proposals and maps out challenges ahead," press release, May 10, 2017, accessed September 19, 2019, https://europa.eu/rapid/press-release_IP-17-1232_en.htm.
96. "Single euro payments area (SEPA)," *European Commission*, accessed September 19, 2019, https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/single-euro-payments-area-sepa_en.
97. "Modernisation of the EU copyright rules," European Commission, July 8, 2019, accessed September 19, 2019, https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules; "Cybersecurity," European Commission, August 23, 2019, accessed September 19, 2019, https://ec.europa.eu/digital-single-market/en/cyber-security.
98. "Notification of a personal data breach to the supervisory authority," Regulation (EU) 2016/679 (General Data Protection Directive), Art. 33 https://gdpr-info.eu/art-33-gdpr/.
99. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
100. Nick Wallace, "EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence" *Center for Data Innovation*, January 25, 2017, accessed September 16, 2019, https://www.datainnovation.org/2017/01/eus-right-to-explanation-a-harmful-restriction-on-artificial-intelligence/.
101. Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America" (Information Technology and Innovation Foundation, January 2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf.
102. "UETA and ESIGN Act," DocuSign.
103. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 96 (2000).
104. Goods and Services Tax Fairness Act of 2019, S. 765 (2019), 115th Cong. (2019).
105. Letter to Speaker Nancy Pelosi and Reps. Steny Hoyer and James Clyburn, Energy and Commerce Republican Members, Nay 22, 2019, accessed September 22, 2019, https://republicans-energycommerce.house.gov/wp-content/uploads/2019/05/NNWG-Letter.pdf.
106. The Ensuring National Constitutional Rights of Your Private Telecommunications (ENCRYPT) Act of 2018, H.R. 6044, 115th Cong. (2018).
107. Daniel Stoller, "Thune Joining Senate Commerce Effort to Craft Data Privacy Bill," *Bloomberg Law*, April 26, 2019, accessed September 19, 2019, https://news.bloomberglaw.com/privacy-and-data-security/thune-joining-senate-commerce-effort-to-craft-data-privacy-bill.
108. Title 12 and 15 focuses on banks and banking and commerce and trade, respectively. 12 U.S.C. §§ 1 et seq., §§ 21 et seq., § 24., §§ 221 et seq., §§ 265-266, 1811-1832., §§ 1461-1470, §§ 1841-1850, §§ 4001-4010, §§ 5201 et seq., §§ 5301 et seq.; 15 U.S.C. §§ 1601 et seq., §§ 8301 et seq.
109. Brake, "National Networks Need National Policies."
110. Importantly, they can only do this if their governing statutes enable this, so Congress may need to get involved to give the requisite authority.
111. U.S. Office of the Comptroller of the Currency, "OCC Begins Accepting National Bank Charter Applications From Financial Technology Companies," press release, accessed July 31, 2018, accessed September 16, 2019, https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-74.html.

112. Joshua Wright, "Regulation in High-Tech Markets: Public Choice, Regulatory Capture, and the FTC," *Federal Trade Commission*, April 2, 2015, https://www.ftc.gov/system/files/documents/public_statements/634631/150402clemson.pdf.
113. North Carolina State Board of Dental Examiners v. Federal Trade Commission, 135 S. Ct. 1101 (2015).
114. Fairness to Contact Lens Consumers Act, Pub.L. 108–164.