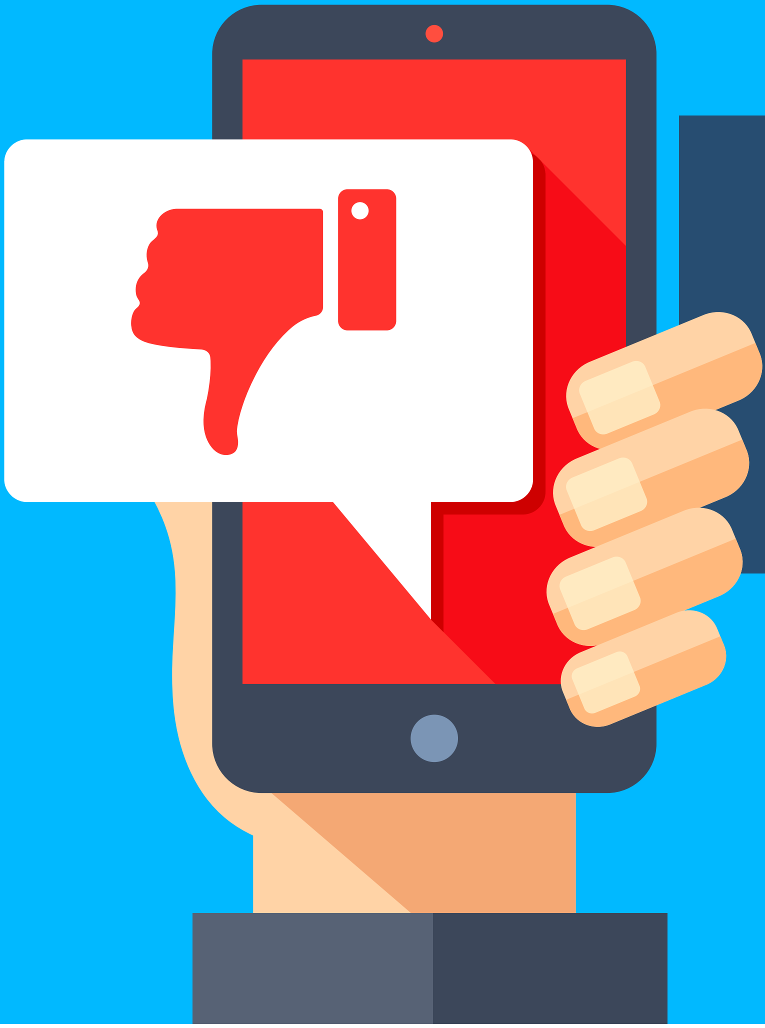
POLICY BRIEF



Deplatforming and Freedom:

A Primer for Policy

Andrea O'Sullivan

Director, Center for Technology & Innovation Policy,
The James Madison Institute

The yearning for freedom is in America's DNA. It always has been: some 200 years ago, the French liberal political philosopher Alexis de Tocqueville examined how the new nation's unique character oriented towards local self-governance and voluntary association[1] in his classic work *Democracy in America*.[2] In contrast to the centralized administration that characterized many European states, the United States of America adopted a federated system where power was limited to as local a level as possible.[3] This intentional separation of powers and retention of rights and authority to the lowest practicable level helped create a democratic culture where government was both responsive to the people and respectful of their desire for liberty.

A lot has changed over the past two centuries, not least of which is the size of our central government, which has regrettably grown considerably. Long gone are the days when government outlays constituted some single-digit percentage of US GDP as it was in the early 20th century; today, gov-

The JAMES MADISON INSTITUTE
Trusted Solutions for a Better Florida

ernment expenditures of almost a quarter of total GDP are more common (to say nothing of our federal debt).[4]

Technology, too, has changed quite a bit, and has allowed us to be much more productive. Total factor productivity, a measure of how much economic output is produced given a set amount of labor and capital, increases in tandem with the returns to technological innovation.[5] Gains from innovation have allowed us to enjoy more material wealth than could have been dreamed of in the days of de Tocqueville.

Yet paradoxically, technologies can be a tool of control just as they can be a means to secure freedom.[6] Indeed, it is no coincidence that the size of government increased at the same time that technologies allowed new scales and records in production.[7] Not only does technology allow more production, which creates more wealth that the government can tax, it also can provide the means for governments to better surveil and clamp down on private activities. For example: it is much easier to spy on digital communications with the click of a computer mouse than it is to physically search millions of pieces of postal mail.

The rise of online platforms extends the paradox that technologies can serve as tools of both liberation and control. Social networking and matching services have made it easier than ever to connect with others, create and share content, and develop our own audiences and even livelihoods online. At the same time, the companies that run these platforms have the power to allow or disallow connections at their own discretion.

Whether exercised on behalf of governments, private activists, or their own whims, platforms' content controls have limited individuals' abilities to connect and communicate in the ways they desire. In extreme cases, users and even competing applications find themselves "deplatformed," or cut off from connectivity, by service providers for actions that are fully legal. Worryingly, deplatforming can occur to stifle certain points of view.

Deplatforming and Conservatives

The problem with deplatforming presents a unique dilemma for conservatives. On the one hand, small government advocates are unsurprisingly wary of any solution that might increase the government's authority over private activities. Online platforms are private businesses that set their own rules, after all. Users are free to leave to join or start a platform more to their liking. And creating a new political power today can easily be wielded against conservative interests tomorrow.

Nevertheless, there is no denying that deplatforming presents a challenge for conservatives. Many voices, ranging from the internationally known to your average Joe, seem to have been unfairly limited on or shut out from platforms. In some cases, it looks like rule by algorithm run amok; perhaps a user was caught in a too-broad net and the platform's appeals process left little explanation or recourse.

In more concerning instances, it may appear that users were targeted merely for the ideological content of their speech—perhaps pro-life,[8] religious,[9] or pro-Second Amendment[10]—that breaks no laws or is not even a clear violation of the platform's terms of service. (Importantly, this is not a partisan issue. Although conservatives may talk about it more—whether because they are targeted more often[11] or merely because they are paying closer attention—left-leaning activists also report being deplatformed for unclear reasons.[12])

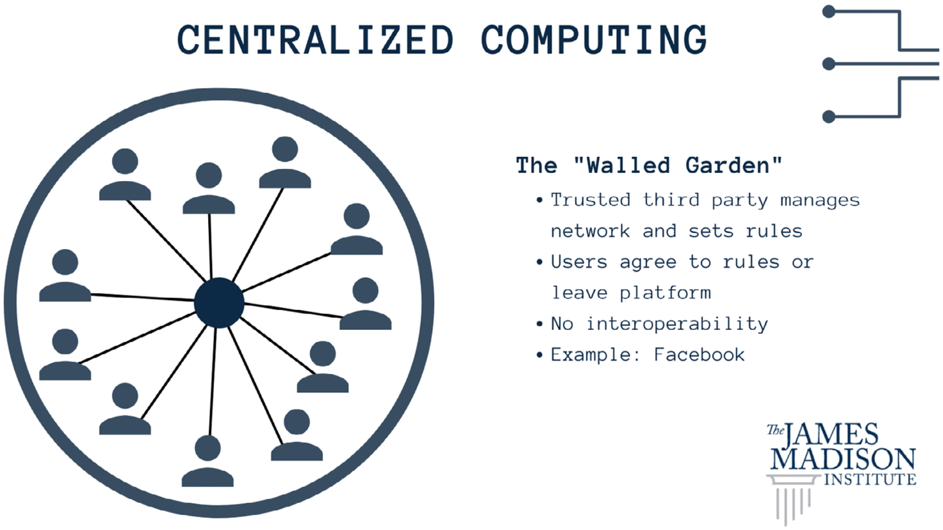
And then there is the problem of the deplatforming of platforms themselves. This is what happened with the more conservative-friendly Parler social networking app. Parler took the advice of tech advocates and built a better alternative for their users. It amassed millions of users and developed a reputation as an open space for conservative commentary and culture. Yet in the days following the unrest at the US Capitol, service providers shut off access for Parler to use critical parts of the internet infrastructure. It was effectively deplatformed for not adopting the specific content moderation policies of leading platforms—suggesting the weakness of the "build your own alternative" argument.

It is tempting to look for a government solution to the problem of deplatforming. Concerned commentators and politicians have proposed remedies ranging from repealing federal liability protections offered under Section 230 of the Communications Decency Act[13] to imposing objectivity or appeal standards on platforms that moderate content for ideological leanings.[14] But as we will see, these options may be either ineffectual or, in the worst case, counterproductive.

This is because the deplatforming problem is not, at its core, a result of policy (although policies may have the effect of making the problem better or worse). Rather, the issue is a predictable consequence of technological design. Technologies that are designed to be *centralized* create conditions where administrators can target users or other platforms. Technologies that are designed to be *decentralized* have no single body that can be targeted to deplatform others; users and services providers decide with whom they want to connect or how. Since the problem itself is technological, only a technological solution can truly alleviate the downsides that deplatforming presents.

This analysis will provide an overview of centralized and decentralized technologies to explain how they work and the trade-offs that these design choices present. Although centralized technologies can be more user-friendly and monetizable than decentralized alternatives, they create central points of control that present privacy, security, and censorship risks. On the other hand, while decentralized platforms present more user freedom and perhaps privacy and security, they often come at the cost of accessibility and present unique, but not insurmountable, challenges for law enforcement.

Policymakers interested in a robust understanding of the debate over platforms and freedom will benefit from a deeper understanding of how design decisions influence technological outcomes. The policies that emanate from such an understanding will therefore be less likely to inadvertently make the platform problem more entrenched. Furthermore, policy leaders will be in a better position to educate the public and serve as early adopters of alternative technologies that reflect their values.



CENTRALIZED COMPUTING

The "Walled Garden"

- Trusted third party manages network and sets rules
- Users agree to rules or leave platform
- No interoperability
- Example: Facebook

The democratic freedom described by de Tocqueville was not forged alone by an enlightened government policy—although constitutional constraints on government certainly allowed it to flourish. It was a reflection of the values and circumstances of America at the time. Although our technological circumstances have certainly changed, our values of free expression and local self-determination are resolute. The challenge is to select the tools that can achieve this freedom online. Adopting and supporting decentralized technologies is an ideologically consistent and, more importantly, *effective* way to achieve a digital freedom that echoes the democratic self-determination of early America.

Centralized vs. decentralized computing

Design choices affect how users can wield tools. When it comes to digital technologies, the structure of a network or platform—namely, the degree of control that is trusted to administrators or users—will determine how actors can engage on that system. One does not need to be a computer scientist to understand the broad contours of centralized networks and decentralized networks, and the effects that these design choices have on people who interact with these networks.

Centralized computing is a network or application that is designed to be operated by a single "trusted third party" or central administrator. The trusted third party assumes discretion over the operation of functions like server management, identity, communications, security, and data. Another word for this arrangement is a "walled garden." This gets at the idea that participating in centralized computing is like visiting a defined property whose owner sets the terms and conditions.

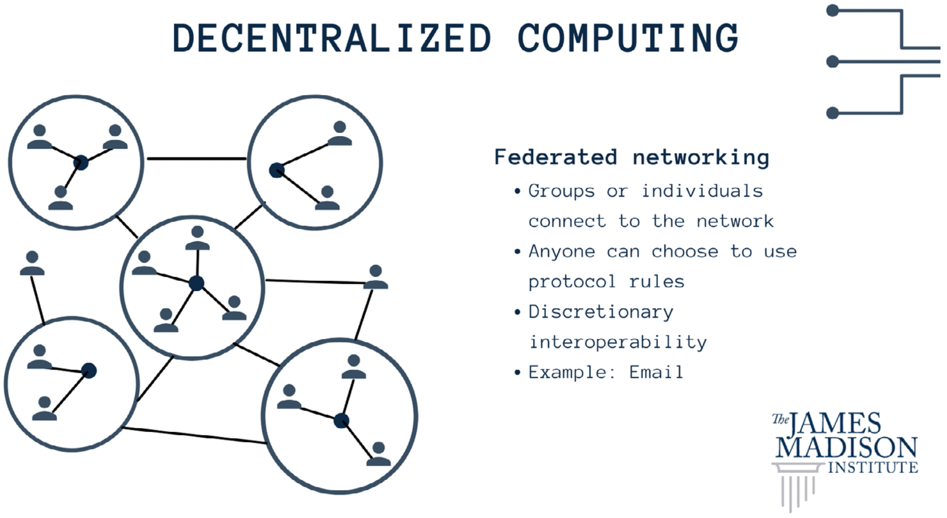
A trusted third party may wield these controls responsibly or incapably. Perhaps the central operator maintains a good system in which many users would like to participate. On the other hand, the administrator may be inadequate. They may frequently allow hackers to steal user data, or allow other guests to run amok, or kick out users if they don't use the right arbitrary language. With centralized computing, the user is at the mercy of the trusted third party. This may not be a problem if there are enough trusted third parties from which to choose, or if it is easy enough for a user to set up their own system. But when users have few alternatives apart from bad trusted third parties, their experience and freedom online will be limited.

Decentralized computing, on the other hand, is a network or application that is designed to be operated by several parties or administrators, with no one body having sole control over the overall system. Decentralized computing may be *federated*—which means that the network is operated by regions of central administration that can decide to connect or disconnect at their discretion—or it may be *distributed*—which means that the network is fully peer-to-peer without any regions of central administration at all; each node or participant is computationally equal to each other.[15]

With decentralized computing, there is no trusted third party that wields controls over the entire system. With a federated system, operators of local servers or applications can enforce their own rules, but only within their own domain, not within the system as a whole. With a distributed system, each participant agrees to certain network rules and runs them to take part in the network.

It is easy enough to understand centralized computing—it is the model that many of us interact with on a daily basis. Because centralized computing grants trusted third parties with considerable control over users, it has unsurprisingly become of interest to powerful parties that would like to benefit from those controls. In other words, what can be politicized will become political. This is why the data and security policies of platforms such as Facebook, Google, Twitter, and Amazon have become so central to policy debates.

Decentralized computing may be a little more difficult to understand when described in the abstract.[16] However, two popular technologies—email and Bitcoin—can help to illustrate what is meant by decentralized networking.


DECENTRALIZED COMPUTING
Federated networking
• Groups or individuals connect to the network
• Anyone can choose to use protocol rules
• Discretionary interoperability
• Example: Email
The JAMES MADISON INSTITUTE

EMAIL: A CASE STUDY IN FEDERATED NETWORKING

Most of us use email every day. We might take it for granted that we are just able to log into our email accounts and send a message to anyone else in the world who has their own operational email account. Comparing the way email works to the way that something like Facebook works helps to illustrate the difference between centralized and federated networking.

There is no "email.com" business that manages the email messages of everyone in the world in the way that Facebook operates its social network. Rather, there are sets of rules—called "protocols"—that anyone can run to take part in the email network. For email, the protocols are called IMAP and POP3. But much of the internet actually runs based on protocols. HTTP, which sets the rules for how our browsers access data on the web, is one. TCP/IP, which governs how computers connect to the internet, is another.

Because email is based on protocols, users have the choice over what service providers they want to use. They can decide to run their own email server, as many people did in the earlier days of the web. Or maybe they use the account provided to them by their employer or ISP (Internet Service Provider). An employer or ISP may run their own servers or contract out to another service provider like Microsoft or Google, which individuals may also seek out on their own. No matter what arrangement an individual selects, all users that follow the protocol rules for the email network will be able to communicate with each other. The network is interoperable.

Compare this to a system like Facebook. You either have an account with Facebook or you don't. There is no way for a person to set up their own server that would allow them to interact with Facebook users or use some other service that is set up for them to do the same.[17] Facebook is sovereign; users are subjects.

People who don't like Facebook for whatever reason can seek out another social network more to their liking, but if no one else is on that network, they probably won't stay very long. Furthermore, as we have seen with alternative centralized networks like Parler, competing networks can be deplatformed by powerful groups. For these reasons, many of the most popular social networks are "sticky" in terms of keeping users on their platform even if users are upset with many platform policies.[18]

As this paper will discuss in the last part of this section, many federated social networking alternatives already exist. Furthermore, legacy social networks, most notably Twitter, have expressed interest in moving to a more federated and interoperable model.[19]

BITCOIN: A CASE STUDY IN DISTRIBUTED NETWORKING

Fully distributed or "peer-to-peer" networks take the logic of decentralization even further. With a distributed network, each actor acts as an autonomous node in the system. The theoretical foundations of distributed computing were laid as a means for dispersed computers to agree to form consensus about the validity of data without trusting any one party.

Originally, distributed computing was conceived as a way for agents to agree on values like time without a central authenticating body.[20] The techniques that overcame longstanding problems in computer science, called the Byzantine General's problem[21] and double-spending problem,[22] eventually came to empower distributed computers to reach consensus on many data types. Users who wish to participate in a distributed network agree to protocol rules and use their computing power to run the network. No one actor can exert force over another in the network; users can merely choose to connect or disconnect from the system.

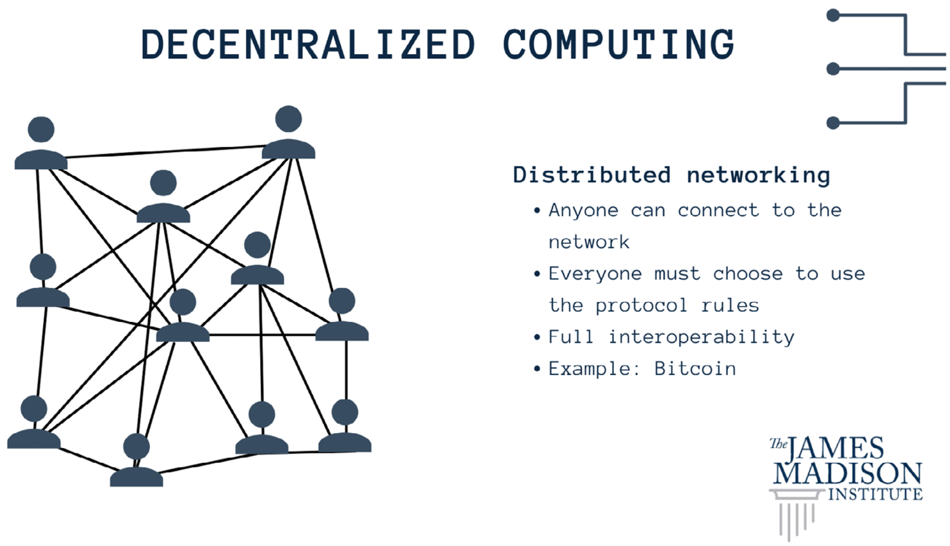
Examples of distributed networks include the file-sharing service BitTorrent and the cryptocurrency Bitcoin. Since most people are at least somewhat familiar with cryptocurrency, it can serve as an example to illustrate peer-to-peer networks. It is especially easy to understand when comparing cryptocurrency to how online transactions used to work.

Before cryptocurrency, if an individual wanted to make a payment online, he or she would first have to register an account with a trusted third party like a bank or a payment processor like PayPal (which was probably connected to a bank), move money to that account, and then tell the trusted third party to move the funds to the trusted third party-managed account of the recipient. Not only can this be time consuming, but it also introduces certain risks to the users. Customer data can and often is hacked and sold on dark markets. Trusted third parties can mismanage or lose funds. Senders or recipients can be blocked from sending money for political or ideological reasons.

Cryptocurrency allows users to send money directly to each other without needing to rely on a trusted third party that can be negligent or targeted. The funds are not moved by a central body, but by the distributed network. With Bitcoin, the network is powered by the computers that decide to connect and run the system. No one computer or group of computers can block or steal transactions. Only the user is in control of their own funds (of course, if they lose their passwords, they can lose their money).

For analytical purposes, it is not necessary to understand exactly how the Bitcoin consensus mechanism, known as proof of work, is designed, although there are many accessible guides for the interested reader.[23] Furthermore, anyone can view the source code and network at any time to verify that the system is working as intended; it has worked exactly as expected for over a decade. All that's required is to understand that distributed systems replace trusted third parties with trust-minimized networks.

A distributed system is quite different from a walled garden like Facebook. Unlike centralized networks, distributed systems are "censorship-resistant." It is virtually impossible to prevent someone from participating in a distributed network; they would have to be physically restrained from accessing a computer. No one can prevent someone from making a transaction on the Bitcoin network. An individual can track down a participant after the fact, and if an individual commits some crime they can be punished, but no one person can prevent another from engaging in a transaction.



DECENTRALIZED COMPUTING

Distributed networking

- Anyone can connect to the network
- Everyone must choose to use the protocol rules
- Full interoperability
- Example: Bitcoin

Bitcoin and distributed digital currencies therefore provide one of the first working solutions to the problem of financial deplatforming. Some activists have found themselves cut off from traditional payment options because of the content of their speech.[24] Being financially deplatformed is unavoidably inconvenient and makes it difficult to earn a living.[25] Consequently, activists have turned to cryptocurrency to be able to earn an income and support themselves.[26] Technologies have applied similar computing concepts to other kinds of possible deplatformings.

OTHER DECENTRALIZED ALTERNATIVES

Distributed systems, like federated systems, provide an attractive non-government solution to the problem of deplatforming. People dissatisfied with the policies of centralized networks can turn to a federated or distributed alternative that removes the potential for a central body to stifle certain points of view. Fortunately, these alternatives are not merely theoretical. Several teams of developers have been building decentralized platforms for years, and they are often just as user-friendly as popular centralized systems.

1. **Fediverse social networking:** One of the biggest challenges with centralized social network platforms is that they leave the user with little choice or power over what content they would like to see. If the platform decides to block certain content, that content is blocked on the platform. Federated social networking options mitigate this by allowing users to interoperate between networks that all run on the same protocol. This is the model of "Fediverse," and it already provides working federated alternatives for services like Twitter (Mastodon), YouTube (PeerTube), and Facebook (Diaspora).

   Recall the distinction between how email functions compared to a platform like Facebook. Fediverse applications work kind of like email but for platforms that are like Facebook. A Fediverse user may use the service server, a third-party server, or run their own server. These servers decide to connect with each other voluntarily. Or if they don't like the way another server is being run, they can disconnect or block that server. No user is simply stuck on a "Facebook" and can either stay and play by the rules, fair or not, or go. They can hop onto an alternative server more to their liking or run their own. And all these servers have the option to interoperate. Or they can block each other if they don't like their policies, so it is a bounded interoperability.

The alternative social network platform Gab provides a good example of how Mastodon instances work, as well as an illustration of how federated networking proves more resilient to deplatforming than a centralized network like Parler. Gab was able to stay online while Parler was deplatformed in part because it is run as a Mastodon instance. Gab runs the Fediverse suite of protocols while maintaining its own servers. Many other Mastodon instances have cut off access to Gab[27] because they dislike Gab's moderation policies, which tend to be lenient of political speech but censorious of sexual content.[28] But other Mastodon users and applications cannot prevent Gab from running as a Mastodon instance. They can only block Gab users from connecting with the services and servers that they control. This model therefore allows censorship-resistance on the protocol level while permitting competition in content moderation on the application level.

2. **Encrypted messaging:** Surveillance—whether by public or private bodies—is a related, but distinct, issue when it comes to deplatforming. Central platforms that have the ability to review communications can use that as a pretext to limit or block certain accounts or content.[29] This information can and has been shared with governments to further their own objectives as well.

   To overcome the possibility of surveillance by central bodies, many have started turning to encrypted messaging applications. Encryption is a mathematical technique to shield the content of communications from anyone but the intended recipient. Encrypted messaging services use a variety of techniques and arrangements to allow private communications among users. Some are free, some are paid, some are open source, and some aren't really all that "encrypted" at all. (For instance, Telegram bills itself as an encrypted chat, but many communications on that platform are not protected by encryption techniques.[30])

   Here, there are also degrees of centralized and decentralized management. A user could choose a free service like Signal, which is open source, yet is tied to a phone number and its servers are managed by a central party with no interoperability. On the other side of the spectrum there is the Matrix/Element project, which is not tied to phone numbers and allows users the option to run their own server. Like the Fediverse, the Matrix protocol allows servers the ability to connect or disconnect with each other as they desire. It is interoperable.
   The move to encrypted messaging platforms is valuable for users who are concerned about privacy. It also benefits those who are concerned that central platforms may review their communications to limit the kinds of connections they are allowed to make on a social network.

3. **Distributed social networking:** Some tech alternatives adopt the blockchain method pioneered by Bitcoin to facilitate dis-

tributed social networking. One good example is the LBRY project, which uses a blockchain to host user videos and pays content creators with its native cryptocurrency.[31] The key innovation is that the blockchain is censorship resistant. Once a video is hosted on the LBRY blockchain, the content cannot be taken down. Other parties then build video explorer applications, which function like a "browser" for the LBRY blockchain, allowing viewers to access the content. It is on the explorer level that content moderation can be applied: explorers can block and remove access to videos that are criminal, for instance. In general, blockchains serve important roles as facilitators of open information. In China, for example, transparency activists have published information about COVID-19 that could not be censored by state agents.[32]

There are other methods to achieve distributed social networking that do not employ a blockchain. One good example is the Urbit project, which provides an open source and peer-to-peer alternative for the entire "computing stack": operating system, server management, identity, and communications.[33] Urbit is one of many decentralized computing projects that aim to route around the central parties that control what users can do with their computers online. Other examples include IPFS, Lokinet, Filecoin, Stacks, and Ethereum.[34]

DOWNSIDES OF DECENTRALIZED NETWORKS

The biggest downside of decentralized networks is that these alternatives lack the user base of controversial central platforms. In the early days of a decentralized network, it may lack users because it is harder to use than centralized platforms. But the bugs eventually get worked out, and many decentralized platforms are just as easy to use as the platforms they seek to replace.

The issue is that decentralized platforms are fighting against the "network effects" enjoyed by centralized incumbents.[35] A social network becomes more valuable as more users join. This is why so many people still have a social network profile even though they might not like the platform: their family and friends are on that network, so they have to stay there to reach them. Network effects are not insurmountable; at one point, MySpace was the industry leader. Obviously, Facebook eventually offered a product that more users preferred. The same could be the case with decentralized alternatives one day. Subsequent sections will discuss various policy concepts that could help these alternatives attract more users and development.

Decentralized networks also present new challenges for law enforcement. Governments prefer central platforms because they offer a "one-stop-shop" for gathering data and evidence. This is a good thing when governments lawfully collect evidence to bring real crimes to justice. It is a problem when governments exploit that access to surveil or oppress political enemies. New alternatives that empower users with interoperability and encryption require new strategies for law enforcement to exert their legitimate powers to effectuate justice. Many computer scientists and lawyers have sketched out ways that law enforcement can update their techniques to bring justice while respecting rights to privacy.[36]

The challenges with centralized platforms

Centralized platforms do provide benefits for users. Because they are controlled, they are often more user-friendly and accessible than decentralized alternatives. Setup is simple, and users don't need to worry about concepts like server management or cryptographic key management. Sometimes, there are "customer service" like arrangements where users can consult with platform associates about things like business listings or content strategy. Central platforms may provide better security than the user might have been able to manage on their own. And if a user likes the platforms' content moderation approach, he or she will appreciate the tailor-made social environment that the platform has cultivated.

But this model also creates challenges. The core one being that it removes choice from the user because the terms of the network are set by the administrator. A user cannot choose to access whatever content he or she wants. The user cannot connect to anyone who is not also on the network—the heavier the restriction, the smaller the possible social graph. And the user cannot manage or protect their own private data; if the administrator has access to it, they can do what they would like with it. This creates concerns for privacy and the potential for government surveillance.

Centralized computing would not be such a big problem if there was sufficient competition in moderation standards that fit the tastes of a diverse population. However, we have seen the rise of a kind of "mono-moderation" culture that tends to take down or deprioritize certain content at the expense of users who wish to see that content. The platform, not the user, is in control. This is not a strictly political concern; platforms that rely on advertiser dollars may tend to promote content in line with the tastes and values of their benefactors rather than what users desire.

Of course, we should not downplay that content moderation often does have a political dimension, and that government and private power centers may use this to their advantage. For instance, a government could lean on a platform to cover up evidence of abuses.[37] Or platforms may intervene to suppress certain content that is unfavorable towards a particular political campaign.[38] The lines between public and private power abuses of centralized computing platforms are very much blurred, which is partially what makes the proper policy approaches so difficult for conservatives who are traditionally opposed or at least apprehensive to government interventions in the economy.

Proposed government interventions on platform moderation

It is understandable that many conservatives have considered government policies to try to alleviate some of the problems that result from centralized platform management. Conservatives are not anarchists. Just because conservatives prefer a system of limited government does not mean that there is *no* role for government. And although the First Amendment is a legal check on *government* powers, the principles of free speech are also an ethos. If it just so happens that *private* groups are the entities restraining the ability to speak, that does not mean there is no issue to be addressed. It means that those advocating for reform need to be creative with their solutions.

However, many of the popular proposals to deal with deplatforming may be ineffective at best or counterproductive at worst. This is because this class of policy does not meaningfully affect the centralized computing arrangement that is the cause of our problems. In fact, many of these policies would have the ironic effect of *strengthening* the position of central platform leaders.

Then there are political considerations. Any policy that places more discretion in the hands of public officials can be targeted or captured by groups that wish to see *more* deplatforming of conservative voices. Given the extreme inequality in influence between progressive and conservative voices in technology, it would be wise for conservatives to resist pushing for more government levers of control that they would be unlikely to wield.

We will now discuss some of the popular proposals offered to remedy the deplatforming issue, and why they may be insufficient to engender the change that proponents hope to see.

IMPOSING GOVERNMENT CONTENT MODERATION CONTROLS

The simplest intervention that political leaders propose to deal with platform moderation is to implement government guidelines on how platforms must handle user-submitted content.

One recent example is Gov. Ron DeSantis and Republican legislative leadership's "Transparency in Technology" proposal.[39] The goals of the reform include giving users the power to opt-out of certain algorithms, stopping frequent changes to the terms of service, requiring platforms to notify users whether they have been censored within 30 days, creating a cause of action for users to sue platforms for arbitrary censorship or inconsistent moderation applications, and empowering the Attorney General to pursue anti-competitive conduct. The proposal would also create specific and unique fines on social media companies that censor political candidates during a campaign.

Republicans are not alone in seeking to legally impose a more attractive content moderation environment on platforms. For those on the left, the complaint is that platforms do not censor *enough*. They would like to expand the definitions of things like "hate speech" so that platforms are legally required to take down more content. (Some platforms welcome this proposed outsourcing of content moderation to leftist groups or governments; it takes the responsibility and blowback out of their hands.[40]) The recently proposed SAFE TECH Act in Congress would legally require platforms to censor what they consider to be "misinformation and discrimination" or risk losing Section 230 protections.[41]. Other academics and journalists call for a government-appointed "reality czar" that would set out the terms of content moderation with social media platforms.[42]

Accordingly, the Florida Legislature's efforts to restrain the problems of censorship and deplatforming are merely a slight counterweight to more powerful and aligned efforts on the federal level. There are questions of legality and federalism:[43] Perhaps the federal government's implied commerce clause authorities would supersede any state's foray into platform moderation controls.[44] But beyond that, a political solution will only last as long as the political environment holds. It would only take a change in state political power for these laws to be reversed. The fundamental challenge is technological. Therefore, it requires a technological solution.

SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

Another commonly proposed solution is to repeal or seriously reform a provision known as Section 230 of the Communications Decency Act. The law protects online platforms from legal liability due to user-submitted content. In other words, a host cannot be sued for the actions of a user on that platform. Rather, injured parties would have to track down the user that submitted the content to attempt a suit.

Critics argue that Section 230 constitutes a "government protection" or even an indirect subsidy to large online platforms that are unaccountable to most users. It is true that limiting or repealing Section 230 would expose platforms to more legal risks. But this would also expose *all* online intermediaries to increased legal risks[45]—even those that choose to moderate their platforms in ways more amenable to critics of Section 230 (which include many on the left who believe platforms allow too much "hate speech" and other content that they find objectionable).[46]

If Section 230 was repealed, we would not likely see an environment that is more friendly to conservative voices. Rather, we might find an online environment scrubbed of any controversial content to limit the risk of being sued. User-submitted content would be quite sterile and only advertiser- or legal department-friendly.

What's worse, repealing Section 230 could ironically empower the biggest platforms at the expense of upstarts. This is because market incumbents have more capital and legal resources at their disposal to navigate the new post-230 world. They already have automatic algorithmic technologies that can take down legally-suspect content, it would be relatively simple for large platforms to adopt such processes to encompass more user content. Smaller platforms would have to undertake this manually, which would require expensive new hires, or invest the resources into building their own sufficiently sophisticated processes. Smaller platforms would also have less of a cushion to weather lawsuits for any content that managed to fall through the cracks.

This path would be a similar effect to how the European Union's General Data Protection Regulation, which aimed to restraint the data practices of big tech platforms, counterproductively served to consolidate their positions.[47] Smaller or non-monetized platforms, which would include many niche websites and forums, would likely choose to just shut down. Repealing Section 230 is therefore more likely to result in a bland and overly-moderated Internet environment than one in which conservative voices are more free to connect. Again, since the challenge of platform moderation is one of technological centralization, only a technological solution of decentralization will bring about the outcomes that conservatives desire.

ANTITRUST AS A REMEDY FOR DEPLATFORMING

The last popular proposal for the government to address the deplatforming problem is to wield antitrust enforcement against large platforms.[48] By breaking up or otherwise limiting the power of big companies, antitrust remedies are thought to be a good way to encourage better moderation policies that are more hospitable to conservative voices.

There are two major problems with this approach. The first is that US antitrust laws are in place to promote competition and consumer welfare, not values like promoting an environment of freedom of speech.[49] There may be good reasons to investigate technology companies for anticompetitive activities that harm consumer welfare. Antitrust suits should be filed on those merits. However, by combining antitrust enforcement with unrelated, but still important, matters of deplatforming, advocates risk muddying up their legal case and perhaps losing on the merits of real problems with anticompetitive behavior.

The second major problem is that deplatforming is not primarily a problem of size, although size may make deplatforming more likely since it is an easier target for powerful groups to wield control. Consider if the government managed to split up Facebook acquisitions, so that WhatsApp and Instagram were separated into their own companies. Would deplatforming and censorship cease? It is unlikely. The companies would still have the same employees and corporate values. They would be no less likely to wield their moderation controls as they had before. In fact, they might tend to be *more* censorious if radical employees find it easier to exert their wills on a smaller company.[50]

More fundamentally, the risk of deplatforming will exist so long as there is a central body that can be targeted to take down certain content. Splitting these companies up would not change the computing design that makes deplatforming possible. Again, because deplatforming is a technological problem, the correct path is to identify a technological solution.

What *can* help

It is easy to point out the problems with government interventions. But this does not mean the problems that those interventions intended to solve—namely, the lack of user freedom to connect and communicate in the ways they desire—magically disappear. It's a real issue that needs adequate solutions.

Solutions exist in the form of decentralized alternatives that route around the potential for central control. The current issue is that many of these alternatives are relatively new and lack users or development. Government should not be in the position of picking winners and losers. But leaders who wish to grapple with the problems of deplatforming should consider how to foster an environment where decentralized alternatives can thrive. There are ways that the government can help to bring these solutions closer to reality. Here are a few steps that Florida policymakers can take to help distributed technologies take flight:

1. **Encourage open source and decentralized technology projects to move and build in Florida**

   The first step is for Florida to keep doing what it has already been doing to attract technologists—particularly the Bitcoin community—to our state. In 2020 Governor Ron DeSantis and the Florida legislature enacted a regulatory sandbox for fintech companies to easily build and experiment in the state.[51] Local leaders such as Miami Mayor Frances Suarez have already begun to leverage this reform in the tech and cryptocurrency community by seeking to promote and adopt these technologies in their municipalities.[52]

   By embracing such policies of "permissionless innovation,"[53] Florida leaders are already attracting the technologists that are most interested in building and applying alternative tech. The Bitcoin community in particular is interested in the potential that decentralized technologies hold for human liberation and connectivity. Continuing to welcome these communities to our state and passing policies that make it easier for them to build is a great way to encourage the kind of technological innovations that can capably address the deplatforming problem.

2. **Where practicable, encourage government offices to educate the public about or adopt open source and decentralized technology projects and standards**

   Policy leaders are more than mere policymakers. They can be influencers, as well. If an elected official decides to stream a video conference on YouTube or Facebook, it will increase the likelihood that people will sign up for or stay on that platform to view and engage with it. It is for this reason that defenders of large tech platforms point out the irony of politicians airing grievances against tech platforms on the very platform that they denigrate.

   Policy leaders could consider experimenting with and creating accounts on some of the decentralized platforms discussed earlier. This is the approach Miami Mayor Suarez has already undertaken: he is exploring ways to pay government employees in cryptocurrency, for example. Other leaders could consider starting social media accounts on decentralized platforms like Mastodon as an alternative to using centralized platforms like Twitter.

   There is a consumer protection element here as well. Florida government already educates the public about important matters regarding safety and consumer welfare. For instance, the Division of Consumer Services offers consumer guides and educational materials on subjects like cryptocurrency, insurance, and financial literacy.[54] Policymakers could consider creating new guides and resources on technology services and products so that users are educated on the issues with different computing applications and which options might work best for them.

   Leaders could consider directing the Florida Department of Management Services to explore, recommend, or implement suitable open source and decentralized technologies as part of Florida's digital infrastructure. The government of Estonia, for instance, has experimented with distributed digital identity systems, which could enhance or replace traditional card-based government ID systems, to some success.[55] As Florida looks to update its identification systems, the kinds of decentralized digital identity systems that are being developed by teams like Microsoft Security provide strong candidates for consideration.[56]

3. **Consider supporting open source and decentralized technology projects and standards in higher education**

   The story of Silicon Valley is partly the story of Stanford University and the US military.[57] Without the academic support, military funding, and early participation of these institutions, the revolution in personal computing might have easily happened elsewhere. This is not to downplay the vision and initiative of the private entrepreneurs that developed and monetized early computing technologies. But having support from well-funded institutions can be the difference between a well-formulated but poorly capitalized dream and, say, the rise of the smartphone.

   Florida government has been long aware of the need to invest in our human capital by ensuring that our university system prepares our students for the jobs of tomorrow. Recent reforms include an emphasis on STEM education and the formation of Florida Polytechnic University to specialize in these domains. Florida universities have also proven nimble in their arrangements with private industry. The University of Florida, for example, has partnered with NVIDIA to create a $70 million artificial intelligence program.[58]

Leadership in Florida could explore ways to encourage our budding ecosystem of cryptocurrency and decentralized technology development by creating focused programs in higher education. Other universities such as the Massachusetts Institute of Technology have developed programs and research centers explicitly dedicated to building these technologies. Not only could the existence of these programs in Florida attract more talent to our state, but it could also have the spillover effect of augmenting our burgeoning cryptocurrency and decentralized tech scene as educational initiatives did in Northern California so many decades ago.

Takeaways for Florida

Florida's leadership has proven to be forward-looking in its embrace of technology. Spearheaded by the legislature and Governor Ron DeSantis, Florida enacted one of the nation's first regulatory sandboxes for cutting-edge financial technology ("fintech") companies. This streamlined regulatory environment should help innovative startups to fast-track their products to market and provide new, affordable, and accessible financial options for Floridians.[59]

Such future-minded policies dovetail nicely with local leaders like Miami's Mayor Francis Suarez, who has embraced the technology sector and engaged with national leaders to bring more innovation to the Sunshine State[60]—Miami was the first municipal government in America to host the Bitcoin white paper on an official public website.[61] The message is clear: if you want to build, come to Miami.[62]

Florida is also looking to improve its "govtech" by updating government websites and processes with state of the art and secure technology. Former legislator and current Florida Chief Information Officer James Grant has made IT modernization a key goal in his tenure. The new Florida Digital Service can help to improve citizen interactions with government IT infrastructure while safely integrating new advancements in digital identity and encryption that can make government processes more efficient and useful.[63]

Florida clearly understands the value of technology and has worked to embrace it in policy. At the same time, conservative leaders understand the threats posed by centralized computing platforms, even if they don't couch it in those terms. Although run by private companies, the design of popular platforms has served to limit users' options for connectivity.

The challenge for policymakers who wish to promote innovation *and* digital self-determination is to create an environment where decentralized alternatives can flourish while remaining vigilant to the controls that centralized applications can wield against users. Furthermore, they must resist the temptation to create new levers of control against users that can merely be exploited by other power centers.

Policymakers who seek to protect Floridians' abilities to connect in the ways they desire online are being good stewards of their constituents. But they must take care that their policy paths do not knock down the great progress we have made in welcoming an innovation culture in Florida. The way to address centralized platforms is not to regulate it to be the way you want. It is to create an environment where innovators can build technologies that make the problem irrelevant.

Building decentralized technologies to route around deplatforming is not only in line with the principles of limited government and free markets and reflective of the kind of uniquely American democratic liberty that Alexis de Tocqueville described some two centuries ago—it is the only way to truly tackle the challenges that centralized computing creates.

Endnotes

[1] Leonard P. Liggio, “Tocqueville and Self-government,” Online Library of Liberty, *Literature of Liberty: A Review of Contemporary Liberal Thought*, Spring 1982, vol. V, no. 1: https://oll.libertyfund.org/page/tocqueville-and-self-government.

[2] Alexis De Tocqueville, *Democracy in America*, New York: G. Dearborn & Co., 1838, https://www.gutenberg.org/files/815/815-h/815-h.htm.

[3] George Carey and James McClellan, eds. *The Federalist*. Indianapolis, IN: Liberty Fund, 2001, https://guides.loc.gov/federalist-papers/full-text.

[4] Historical Tables, “Table 1.1—Summary of Receipts, Outlays, and Surpluses or Deficits (-): 1789–2025,” and “Table 1.2—Summary of Receipts, Outlays, and Surpluses or Deficits (-) as Percentages of GDP: 1930–2025,” *Office of Management and Budget*, accessed February 18, 2021, https://www.whitehouse.gov/omb/historical-tables/.

[5] Robert Shackleton, “Total Factor Productivity Growth in Historical Perspective,” *Congressional Budget Office*, May 2013, https://www.cbo.gov/sites/default/files/113th-congress-2013-2014/workingpaper/44002_TFP_Growth_03-18-2013_1.pdf.

[6] Eli Dourado, “Technologies of Control and Resistance,” November 4, 2011, https://elidourado.com/blog/technologies-of-control-and-resistance/.

[7] Tyler Cowen, “Does Technology Drive The Growth of Government?” *Working Paper*, June 22, 2009, http://www.bcaplan.com/Cowentech.pdf.

[8] Senator Josh Hawley, “Senators Hawley, Cruz, Cramer, and Braun Blast Facebook for Censoring Pro-Life Content.” https://www.hawley.senate.gov/senators-hawley-cruz-cramer-and-braun-blast-facebook-censoring-pro-life-content.

[9] Jonathon Liedl, “Big Tech’s Big Bias: Religious Conservatives Face ‘Scary Pattern’ of Censorship.” *National Catholic Register*, https://www.ncregister.com/news/big-tech-s-big-bias-religious-conservatives-face-scary-pattern-of-censorship.

[10] Austin Yack, “Why Is Facebook Censoring Pro-Second Amendment Pages?,” *National Review,* August 9, 2016. https://www.nationalreview.com/2016/08/facebook-censors-pro-gun-rights-pages/.

[11] This could be for many reasons, including because platforms seek to moderate conservative voices more stringently or because conservatives are overrepresented on a platform.

[12] Andrea Damon “Facebook Purges Left-Wing Pages and Individuals,” *World Socialist Web Site*, https://www.wsws.org/en/articles/2021/01/23/pers-j23.html.

[13] Senator Josh Hawley. “Senator Hawley Introduces Legislation to Amend Section 230 Immunity for Big Tech Companies,” https://www.hawley.senate.gov/senator-hawley-introduces-legislation-amend-section-230-immunity-big-tech-companies.

[14] “Governor Ron DeSantis, Florida House Speaker Chris Sprowls and Senate President Wilton Simpson Highlight Proposed Legislation to Increase Technology Transparency in Florida,” https://www.flgov.com/2021/02/02/governor-ron-desantis-florida-house-speaker-chris-sprowls-and-senate-president-wilton-simpson-highlight-proposed-legislation-to-increase-technology-transparency-in-florida/.

[15] Leslie Lamport, “Time, Clocks, and the Ordering of Events in a Distributed System,” *Communications of the ACM 21*, no. 7, pgs. 558–65, July 1, 1978, https://doi.org/10.1145/359545.359563.

[16] “Ecosystem Review,” *Blue Sky*, January 2021, https://matrix.org/_matrix/media/r0/download/twitter.modular.im/981b258141aa0b197804127cd2f7d298757bad20.

[17] Curtis Yarvin, “How to Regulate the Tech Platforms,” *Gray Mirror*, November, 19th 2020, https://graymirror.substack.com/p/how-to-regulate-the-tech-platforms.

[18] Nicholas Economides, “The Economics of Networks,” *International Journal of Industrial Organization* 14, no. 6 (October 1, 1996): 673–99. https://doi.org/10.1016/0167-7187(96)01015-6.

[19] Adi Robertson, “Twitter Is Funding Research into a Decentralized Version of Its Platform,” *The Verge*, December 11, 2019. https://www.theverge.com/2019/12/11/21010856/twitter-jack-dorsey-bluesky-decentralized-social-network-research-moderation.

[20] Edsger Dijkstra, “Self-Stabilizing Systems in Spite of Distributed Control,” *Burroughs Corporation*, http://homepage.divms.uiowa.edu/~ghosh/ssDijkstra.pdf.

[21] Leslie Lamport, “The Byzantine Generals Problem,” *SRI International*, July 1982. https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf.

[22] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf.

[23] Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 1st edition. Sebastopol CA: O’Reilly Media,

Endnotes (Cont.)

2014.

24 “Financial Censorship,” *Electronic Frontier Foundation*, https://www.eff.org/issues/financial-censorship.

25 Andrea O’Sullivan, “Proposed Banking Rule Change Would Upend Oppressive ‘Operation Chokepoint’ Tactics,” *Reason*, December 8, 2020. https://reason.com/2020/12/08/proposed-banking-rule-change-would-upend-oppressive-operation-chokepoint-tactics/.

26 Roger Huang, “How Bitcoin And WikiLeaks Saved Each Other,” *Forbes*, https://www.forbes.com/sites/rogerhuang/2019/04/26/how-bitcoin-and-wikileaks-saved-each-other/.

27 “Statement on Gab’s fork of Mastodon,” Mastodon blog, July 4, 2019, https://blog.joinmastodon.org/2019/07/statement-on-gabs-fork-of-mastodon/.

28 Gab Terms of Service, accessed February 23, 2021, https://gab.com/about/tos.

29 Ashley Carman, “Instagram Announces Tougher Consequences for Hate Speech in Direct Messages,” *The Verge*, February 10, 2021, https://www.theverge.com/2021/2/10/22276491/instagram-direct-message-hate-speech-account-disabled-policy.

30 Douglas Crawford, “7 WhatsApp Alternatives That Won’t Share Your Data with Facebook,” *ProtonMail Blog*, February 15, 2021, https://protonmail.com/blog/whatsapp-alternatives/.

31 Andrea O’Sullivan, “The Best Way for Florida to ‘Take on Big Tech’ Is to Keep Welcoming the Crypto Community,” *Reason*, February 23, 2021, https://reason.com/2021/02/23/the-best-way-for-florida-to-take-on-big-tech-is-to-keep-welcoming-the-crypto-community/.

32 Roger Huang, “Chinese Netizens Use Ethereum To Avoid China’s COVID-19 Censorship,” *Forbes*, https://www.forbes.com/sites/rogerhuang/2020/03/31/chinese-netizens-use-ethereum-to-avoid-chinas-covid-19-censorship/.

33 Andrea O’Sullivan, “Can Urbit Reboot Computing?,” *Reason*, June 21, 2016. https://reason.com/2016/06/21/can-urbit-transform-the-internet/.

34 Zach Weissmueller, “How To Fight Deplatforming: Decentralize,” *Reason*, February 17, 2021. https://reason.com/video/2021/02/17/how-to-fight-deplatforming-decentralize/.

35 Nicholas Economides, “The Economics of Networks,” *International Journal of Industrial Organization* 14, no. 6 (October 1, 1996): 673–99. https://doi.org/10.1016/0167-7187(96)01015-6.

36 Nancy Gertner, et al, “Don’t Panic: Making Progress on the ‘Going Dark’ Debate,” *Berkman Center Research Publication*, 2016, https://dash.harvard.edu/handle/1/28552576.

37 Andrea O’Sullivan, “Shadow-Censorship on Social Media Sparks New Concerns for Open-Internet Advocates,” *Reason*, October 27, 2015. https://reason.com/2015/10/27/shadow-censorship-on-social-media/.

38 Noah Manskar, “Twitter, Facebook Censor Post over Hunter Biden Exposé.” New York Post, October 14, 2020, https://nypost.com/2020/10/14/facebook-twitter-block-the-post-from-posting/.

39 Twitter. https://twitter.com/flgopmajority/status/1356629127621734403.

40 *See, for example*: Mark Zuckerberg, “Opinion | Mark Zuckerberg: The Internet Needs New Rules. Let’s Start in These Four Areas,” *Washington Post*, March 30, 2019, https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

41 “To Amend Section 230 of the Communications Act of 1934 to Reaffirm Civil Rights, Victims’ Rights, and Consumer Protections.” 117TH CONGRESS 1ST SESSION, n.d. https://www.warner.senate.gov/public/_cache/files/4/f/4fa9c9ba-2b34-4854-8c19-59a0a9676a31/66DECFBC0D6E6958C2520C3A6A69EAF6.safe-tech-act---final.pdf.

42 Kevin Roose, “How the Biden Administration Can Help Solve Our Reality Crisis,” *The New York Times*, February 2, 2021, https://www.nytimes.com/2021/02/02/technology/biden-reality-crisis-misinformation.html.

43 Scott Shackford, “Florida Gov. Ron DeSantis Wants $100,000 Fines for Social Media Companies That Deplatform Politicians,” *Reason*, February 4, 2021.

44 Jennifer Huddleston, “Potential Constitutional Conflicts in State and Local Data Privacy Regulations,” *Regulatory Transparency Project*, December 2 2019, https://regproject.org/paper/potential-constitutional-conflicts-in-state-and-local-data-privacy-regulations/.

45 Karl Herchenroeder, “Parler Executive Defends Section 230, Platform Moderation Practices,” *Communications Daily*, December 7, 2020, https://communicationsdaily.com/news/2020/12/07/parler-executive-defends-section-230-platform-moderation-practic-

Endnotes (Cont.)

es-2012040050.

46 Daisuke Wakabayashi, "Legal Shield for Websites Rattles Under Onslaught of Hate Speech," *The New York Times*, August 6, 2019, https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html.

47 Nick Kostov, "GDPR Has Been a Boon for Google and Facebook," *Wall Street Journal*, June 17, 2019, https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219.

48 Angelica Stabile, "Ted Cruz: Facebook, Twitter, Google Collectively Pose 'Single Greatest Threat' to Free Speech in America," *FOXBusiness*, November 17, 2020. https://www.foxbusiness.com/technology/ted-cruz-facebook-twitter-google-collectively-pose-single-greatest-threat-to-free-speech-in-america.

49 Joshua D. Wright, et al, "Requiem for a Paradox: The Dubious Rise and Inevitable Fall of Hipster Antitrust," *Arizona State Law Journa*l 51 (2019): 293.

50 Indeed, big tech companies have found themselves at the mercy of angry employees on issues ranging from content moderation to government contracts. *See*: Nitasha Tiku, "Why Tech Worker Dissent Is Going Viral," *WIRED*, July 29th, 2018, https://www.wired.com/story/why-tech-worker-dissent-is-going-viral/.

51 "CFO Press Release 6/30/2020 CFO Jimmy Patronis Applauds Governor Ron DeSantis on Signing FinTech Legislation, House Bill 1391," https://www.myfloridacfo.com/sitePages/newsroom/pressRelease.aspx?ID=5578.

52 Joey Flechas, "Miami Votes to Study Using Bitcoin for Employee Salaries and Payments to City Hall." *Miami Herald*, February 12, 2021, https://www.miamiherald.com/news/business/technology/article249202060.html.

53 Andrea O'Sullivan, "Let's Fully Embrace 'Permissionless Innovation,'" *Florida Politics*, June 1, 2020. https://floridapolitics.com/archives/337081-andrea-osullivan-lets-fully-embrace-permissionless-innovation.

54 "Division of Consumer Services." https://www.myfloridacfo.com/division/consumers/.

55 Metadium, "How Estonia Is Pioneering the Digital Identity Space," *Medium*, July 16, 2019. https://medium.com/metadium/how-estonia-is-pioneering-the-digital-identity-space-4008c709fbb8.

56 "Decentralized Identity – Own Your Digital Identity." https://www.microsoft.com/en-us/security/business/identity/own-your-identity.

57 Stephen Mihm, "How the Department of Defense Bankrolled Silicon Valley," *Stanford Engineering*, July 9, 2019. https://systemx.stanford.edu/news/2019-07-09-000000/how-department-defense-bankrolled-silicon-valley;"The Interdependency Of Stanford And Silicon Valley," *TechCrunch*, https://social.techcrunch.com/2015/09/04/what-will-stanford-be-without-silicon-valley/.

58 Steve Orlando, "UF Announces $70 Million Artificial Intelligence Partnership with NVIDIA," *University of Florida*, July 21, 2020, https://news.ufl.edu/2020/07/nvidia-partnership/.

59 Andrea O'Sullivan, "Expanding Regulatory Sandboxes to Fast-Track Innovation," *James Madison Institute*, January 28, 2021. https://www.jamesmadison.org/expanding-regulatory-sandboxes-to-fast-track-innovation/.

60 "'Unique Opportunity': Suarez Speaks With Elon Musk About Tunnels Under Miami," *NBC 6 South Florida*, February 5, 2021. https://www.nbcmiami.com/news/local/unique-opportunity-suarez-speaks-with-elon-musk-about-tunnels-under-miami/2376498/.

61 Danny Nelson, "Miami Uploads Bitcoin White Paper to Municipal Website," *CoinDesk*, January 27, 2021. https://www.coindesk.com/miami-bitcoin-white-paper.

62 Sophia Kunthara, "Why Miami Is The Next Hot Tech Hub: 'This Is Not A Retirement Decision.'" *Crunchbase News*, January 5, 2021, https://news.crunchbase.com/news/why-miami-is-the-next-hot-tech-hub/.

63 Bill to Reorganize Florida IT Awaits Governor's Signature," *GovTech*, https://www.govtech.com/computing/Bill-to-Reorganize-Florida-IT-Awaits-Governors-Signature.html.

The JAMES MADISON INSTITUTE
Trusted Solutions for a Better Florida

✉ The James Madison Institute
The Columns
100 North Duval Street
Tallahassee, FL 32301

☎ 850.386.3131

www.jamesmadison.org

Stay Connected
The James Madison Institute
@JmsMadisonInst
youtube.com/user/JamesMadisonInstitut
flickr.com/photos/jmsmadisoninst
pinterest.com/jmsmadisoninst