FREE SPEECH FUTURES

Protocols, Not Platforms

A Technological Approach to Free Speech

By Mike Masnick

KNIGHT
FIRST AMENDMENT
INSTITUTE
at Columbia University

This essay is part of the Knight First Amendment Institute's essay series, Free Speech Futures. Authors were asked to envision new approaches to First Amendment doctrine and to online content moderation. The eight essays in the series consider the future of free speech along two dimensions. The first set proposes new interpretations and applications of the First Amendment by courts to meet 21st century pressures and challenges. The second offers new strategies and technologies to improve the quality and health of the online speech environment.

The Free Speech Futures essay series was conceptualized and edited by Jamal Greene, Dwight Professor of Law at Columbia Law School, during his tenure as the Knight Institute's Senior Visiting Research Scholar. The Knight Institute's Research Director Katy Glenn Bass and other Institute staff provided additional editing and review.

The full series is available at knightcolumbia.org/research/

Protocols, Not Platforms

A Technological Approach to Free Speech

By Mike Masnick

INTRODUCTION

AFTER A DECADE OR SO of the general sentiment being in favor of the internet and social media as a way to enable more speech and improve the marketplace of ideas, in the last few years the view has shifted dramatically—now it seems that almost no one is happy. Some feel that these platforms have become cesspools of trolling, bigotry, and hatred.[1] Meanwhile, others feel that these platforms have become too aggressive in policing language and are systematically silencing or censoring certain viewpoints.[2] And that's not even touching on the question of privacy and what these platforms are doing (or not doing) with all of the data they collect.

The situation has created something of a crisis, both inside and outside of these companies. The companies are constantly struggling to deal with their new positions as arbiters of truth and kindness online, despite historically promoting themselves as defenders of free speech. Meanwhile, politicians from the two major political parties have been hammering these companies, albeit for completely different reasons. Some have been complaining about how these platforms have potentially allowed

for foreign interference in our elections.[3] Others have complained about how they've been used to spread disinformation and propaganda.[4] Some have charged that the platforms are just too powerful.[5] Others have called attention to inappropriate account and content takedowns,[6] while some have argued that the attempts to moderate discriminate against certain political viewpoints.[7]

What is clear is that there is no simple solution to these challenges, and most of the ones that are normally presented tend not to deal with the reality of the problems or to understand the technical and societal challenges that likely make them impossible.

Some have argued for much greater policing of content online, and companies like Facebook, YouTube, and Twitter have talked about hiring thousands to staff up their moderation teams.[8] On the other side of the coin, companies are increasingly investing in more and more sophisticated technology help, such as artificial intelligence, to try to spot contentious content earlier in the process.[9] Others have argued that we should change Section 230 of the Communications Decency Act (CDA), which gives platforms a free hand in determining how they moderate (or how they don't moderate).[10] Still others have suggested that there should be no moderation allowed at all—at least for platforms of a certain size—such that they are deemed part of the public square.[11]

As this article will attempt to highlight, most of these solutions are not just unworkable; many of them will make the initial problems worse or will have other effects that are equally pernicious.

This article proposes an entirely different approach—one that might seem counterintuitive but might actually provide for a workable plan that enables more free speech, while minimizing the impact of trolling, hateful speech, and large-scale disinformation efforts. As a bonus, it also might help the users of these platforms regain control of their privacy. And to top it all off, it could even provide an entirely new revenue stream for these platforms.

That approach: build protocols, not platforms.

To be clear, this is an approach that would bring us *back* to the way the internet used to be. The early internet involved many different protocols—instructions and standards that anyone could then use to

build a compatible interface. Email used SMTP (Simple Mail Transfer Protocol). Chat was done over IRC (Internet Relay Chat). Usenet served as a distributed discussion system using NNTP (Network News Transfer Protocol). The World Wide Web itself was its own protocol: HyperText Transfer Protocol, or HTTP.

In the past few decades, however, rather than building new protocols, the internet has grown up around controlled platforms that are privately owned. These can function in ways that appear similar to the earlier protocols, but they are controlled by a single entity. This has happened for a variety of reasons. Obviously, a single entity controlling a platform can then profit off of it. In addition, having a single entity can often mean that new features, upgrades, bug fixes, and the like can be rolled out much more quickly, in ways that would increase the user base.

Indeed, some of the platforms today are *leveraging* existing open protocols but have built up walls around them, locking users in, rather than merely providing an interface.[12] This actually highlights that there is not an either/or choice here between platforms and protocols but rather a spectrum. However, the argument presented here is that we need to move much more to a world of open protocols, rather than platforms.

Moving to a world where protocols and not proprietary platforms dominate would solve many issues currently facing the internet today. Rather than relying on a few giant platforms to police speech online, there could be widespread competition, in which anyone could design their own interfaces, filters, and additional services, allowing whichever ones work best to succeed, without having to resort to outright censorship for certain voices. It would allow end users to determine their own tolerances for different types of speech but make it much easier for most people to avoid the most problematic speech, without silencing anyone entirely or having the platforms themselves make the decisions about who is allowed to speak.

In short, it would push the power and decision making out to the ends of the network, rather than keeping it centralized among a small group of very powerful companies.

At the same time, it would likely lead to new, more innovative features as well as better end-user control over their own data. Finally,

it could help usher in a series of new business models that don't focus exclusively on monetizing user data.

Historically, the internet moved more and more to a world of centralized platforms over decentralized protocols due, in part, to the incentive structure under the old internet. Protocols were difficult to monetize. Because of that, it was difficult to keep them updated and to provide new features in a compelling way. Companies often came in and "took over," creating a more centralized platform, adding on their own features (and incorporating their own business models). They were able to put more resources toward those platforms (and business models), creating a virtuous cycle (and some number of locked-in users) for the platform.

However, that has brought its own difficulties. With control has come demands for responsibility, including ever greater policing of the content hosted on these platforms. It has also created concerns about filter bubbles and bias.[13] In addition, it has created a dominance of a few internet companies, and that (quite reasonably) makes many people uncomfortable.[14]

Moving back to a focus on protocols over platforms can solve many of these problems. And other recent developments suggest that doing so could overcome many of the earlier pitfalls of protocol-based systems, potentially creating the best of all words: useful internet services, with competition driving innovation, not controlled solely by giant corporations, but financially sustainable, providing end users with more control over their own data and privacy—and providing mis- and disinformation far fewer opportunities to wreak havoc.

THE EARLY PROBLEMS WITH PROTOCOLS AND WHAT PLATFORMS DO WELL

WHILE THE EARLY INTERNET was dominated by a series of protocols, rather than platforms, the limitations of those early protocols show why platforms came to dominate. There are many different platforms, each one coming with its own set of reasons why they were successful for a time and failed (or not), but to help illustrate the issues discussed here, we'll limit our comparison to Usenet and Reddit.

Conceptually, both Usenet and Reddit are quite similar. Both involved a set of forums generally organized around a particular topic. On Usenet, these were called newsgroups. On Reddit, they are subreddits.[15] Each newsgroup or subreddit tended to have moderators who were empowered to put different rules in place. Users could post new posts within each group, leading to threaded replies from others in the group, creating an approximation of a discussion.

However, Usenet was an open protocol (technically, the Network News Transfer Protocol, or NNTP) that anyone could tap into, using a

variety of different applications. Reddit is a centralized platform controlled entirely by a single company.

To access Usenet, you initially needed a special newsreader client app (of which there were several) and then you would need to access a Usenet server. Many internet service providers originally offered their own (when I first got on the internet in 1993, I used Usenet via a news server at my university, along with the Usenet reader the university provided). As the web became more popular, more organizations attempted to provide a web front end to Usenet. In the early days this space was dominated by Deja News Research Service, which provided one of the first web interfaces to Usenet; it later added a bunch of additional features, including (most helpfully) a comprehensive search engine.

While Deja News experimented with a variety of different business models, eventually its search was shut down. Google acquired the company in 2001[16], including its Usenet archives, which it used as a key part of Google Groups (which still offers email-style mailing lists that are exclusive to the Google platform, and a web interface to much of Usenet and its newsgroups).

Much of Usenet was complicated and unclear (especially prior to the widespread advent of web interfaces). An early joke on Usenet was that every September the service would be filled with confused "newbies," inevitably college freshman who had just been granted new accounts and had little idea of the prevailing practices and proper etiquette involved in using the service. September, then, tended to be the time during which a lot of old-timers found themselves frustratingly "correcting" the behavior of these new entrants until they conformed to the system's norms.

In the same spirit, the period after September of 1993 has been memorialized by old-school Usenet aficionados as "the September that never ended" and "Eternal September." That was the moment that the proprietary platform America Online (AOL) opened its doors to Usenet, leading to a massive influx of users who weren't so easily tamed.[17]

Since there were many different Usenet servers, the content is not centrally hosted but propagates across the various servers. This has advantages and disadvantages, including that different servers can treat different content in different ways. Not every Usenet server has to host

every group. But it also means that there is not a central authority to deal with disruptive or trollish activity. However, certain servers could choose to block certain newsgroups, and end users could use tools such as kill files to filter out a variety of unwanted content based on criteria that the user themselves chose.[18]

Another major disadvantage to the original Usenet was that it was not particularly adaptive or flexible, especially in terms of larger-scale changes. As it was a decentralized set of protocols, there was an involved consensus process that required agreement from a wide range of parties before any changes to the protocol could be implemented. Even smaller changes often required considerable work and even then were not always recognized universally. Starting a new newsgroup was a fairly involved process. For certain hierarchies there was an approval process, but other "alt" categories were much easier to set up (although whether or not all Usenet servers would *carry* that board was not guaranteed).[19] By comparison, it is easy to set up a new subreddit. Reddit has a product and engineering team that can make any changes it desires—but the userbase has far less say in how those changes occur.

Perhaps the largest problem with the old system was the lack of an obvious business model. As the death of Deja News showed, it had never been particularly profitable to run a Usenet server. Over time, there has been a growth of "professional" Usenet servers that require payment to access, but those tended to come about much later, are not that large compared to an internet platform like Reddit, and are generally considered to be focused on trading in infringing content.[20]

THE CURRENT PROBLEMS OF BIG PLATFORMS

IN THE LAST TWO DECADES, the rise of internet platforms—Facebook, Twitter, YouTube, Reddit, and others—have more or less displaced the protocol-based systems used previously. With the platforms, there is a single (usually for-profit) company that runs the services for end users. These services tend to be funded first by venture capital and then by advertising (often highly targeted).

The platforms are all built on the World Wide Web and tend to be accessed through a traditional internet web browser or, increasingly, a mobile device app. The benefits of building a service as a platform are fairly obvious: the owner has ultimate control over that platform and thus is much better positioned to monetize the platforms via advertising of some form (or other ancillary services). This does, however, incentivize these platforms to acquire an ever increasing amount of data from their users to better target them.

This has resulted in reasonable concerns and pushback from both users and regulators, who are concerned that platforms are not playing fairly or not properly "protecting" the end-user data they have been collecting.[21]

A second problem facing the largest platforms today is that as they have become larger and more central to everyday lives, there is growing concern directed at the operators of these platforms about the content that they have enabled to be posted—as well as the responsibilities those operators might have in policing or blocking that content.[22] They have faced increasing pressure from both users and politicians to police that content more proactively.[23] In some cases, laws have been passed that more explicitly require platforms to delete certain content, slowly chipping away at the earlier immunity (e.g., the Communications Decency Act, Section 230, in the U.S., or the E-Commerce Directive in the EU) that many platforms enjoyed over their moderation choices.

Because of this, platforms have felt reasonably compelled not only to be more proactive but also to testify before various legislative bodies, to hire thousands of employees as potential content moderators, and to invest heavily in moderation technology. Yet even with these regulatory mandates and human and technical investments, it is still not clear that any platform can actually do a "good" job of moderating content at scale.

Part of the problem is that any platform moderation decision is going to upset someone. Obviously, those whose content was moderated tend not to be happy about it, but the same is true of others who wished to see or share that content. At the same time, in many cases a decision *not* to moderate content can also upset people. Currently, the platforms are receiving quite a lot of criticism for their moderation choices, including accusations (mostly evidence-free, to be sure) that political bias is driving those content moderation choices. As the platforms face pressure to take on more responsibility, every choice concerning content moderation they make puts them in a bind. Remove disputed content—and anger those who created it or support it; refrain from removing disputed content—and anger those who find it problematic.

This puts the platforms in a no-win position. They can keep throwing more and more money at the problem and continue to talk to the public and politicians, but it is unclear how this ever ends with enough people being "satisfied." It is not difficult on any given day to find people upset with platforms like Facebook, Twitter, and YouTube when they fail to take down certain content—who can immediately be replaced by those

upset with the platforms when they eventually do take down that content.

This setup is frustrating for everyone involved, and it's unlikely to get better anytime soon.

PROTOCOLS TO THE RESCUE

In this article, I am proposing that we return to a world of protocols dominating the internet, rather than platforms. There is reason to believe that moving to a system of protocols could solve many of the problems associated with platforms today and that it could be done while minimizing the problems that were inherent to protocols a few decades ago.

While there is no silver bullet, a system of protocols could serve to do a better job of protecting both user privacy and free speech, while at the same time minimizing the impact of abusive behavior online and creating new and compelling business models that are more aligned with user interests.

The key to making this work is that while there would be specific protocols for the various types of platforms we see today, there would then be *many competing interface implementations* of that protocol. The competition would come from those implementations. The lowered switching costs of moving from one implementation to another would create less lock-in, and the ability for anyone to create their own interface and get

access to all of the content and users on the underlying protocol makes the barriers to entry for competition drastically lower. You don't need to build an entirely new Facebook if you already have access to everyone making use of the "social network protocol" and just provide a different, or better, interface to it.

An example of this is already seen, to some extent, in the email space. Built on open standards such as SMTP, POP3 and IMAP,[24] there are many different implementations of email. Popular email systems in the 1980s and 1990s relied on a client-server setup whereby the service provider (whether a commercial internet service provider, a university, or an employer) would host the email only briefly on a server, until they were downloaded to the user's own computer via some client software, like Microsoft Outlook, Eudora, or Thunderbird. Or, users could access that email via a text interface, such as Pine or Elm.[25]

The late 1990s saw the rise of web-based email, first with Rocketmail (eventually purchased by Yahoo, becoming Yahoo Mail) and Hotmail (purchased by Microsoft, years later becoming Outlook.com). Google introduced its own offering, Gmail, in 2004, which kicked off a new round of innovation, as Gmail offered vastly more storage space for email as well as a significantly faster user interface.[26]

However, because of these open standards, there is a great deal of flexibility. A user can use a non-Gmail email address within the Gmail interface. Or he or she can use a Gmail account with an entirely different client, such as Microsoft Outlook or Apple Mail.[27] On top of that, it's possible to create new interfaces on top of Gmail itself, such as with a Chrome extension.[28]

This setup has many advantages for the end user. Even if one platform—like Gmail—becomes much more popular in the marketplace, the costs of switching are much lower. If a user does not like how Gmail handles certain features or is concerned about Google's privacy practices, switching to a different platform is much easier, and the user does not lose access to all of his or her old contacts or the ability to email anyone else (even those contacts that remain Gmail users).

Notice that this flexibility serves as a strong incentive on Google's part to make sure that Gmail treats its users well; Google is less likely

to take actions that might lead to a rapid exodus. This is different than a fully proprietary platform such as Facebook or Twitter, where leaving those platforms means that you no longer are in communication in the same way with the people there and can no longer easily access their content and communications. With a system like Gmail, it is easy to export contacts and even legacy emails and simply begin again with a different service, without losing the ability to remain in contact with anyone.

In addition, it opens up the competitive environment much more. Even as Gmail is an especially popular email service, others are able to build up significant email services—like Outlook.com or Yahoo Mail—or to create successful startup email services that target different markets and niches—like Zohomail or Protonmail.[29] It also opens up other services that can build on top of the existing email ecosystem, with less fear of a being reliant on a single platform that might shut them out. For example, both Twitter[30] and Facebook[31] have a tendency to switch product directions and to cut off third-party apps, but in the email space, there's a thriving market of services and companies like Boomerang, SaneBox, and MixMax, each of which provides additional services that can work on a variety of different email platforms.[32]

The end result is more competition to make the service better, both between and within email services, and strong incentives to keep the major providers acting in their users' best interests, since the significantly lower lock-in gives those users the option to leave.

Protecting Free Speech, but Limiting Impact of Abusive Behavior

Perhaps the most controversial part in discussions about content moderation is what to do about "abusive" behavior. Nearly everyone recognizes that there is such behavior online and that it can be destructive, but there is no agreement on what it actually includes. Behavior that has concerned people can fall into lots of different categories, from harassment to hate speech to threats to trolling to obscenity to doxxing to spam and more. But none of those categories has a comprehensive definition, and much of it is in the eye of the beholder. For example, one person's attempt to express an opinion strongly can be seen by the recipient as

harassment. Neither party may be "wrong" per se, but leaving it up to each platform to adjudicate such things is an impossible task, especially when dealing with hundreds of millions of pieces of content per day.

Currently, platforms are the ultimate centralized authority in dealing with these questions. Many have tackled the problem with increasingly complex bodies of internal "law" (whose "rulings" are often not evident to end users), which is then handed off to a large number of employees (frequently outsourced with relatively low wages), who are given very little time to make judgment calls on thousands of pieces of content.[33]

Under such a system, both Type I ("false positive") and Type II ("false negative") errors are not only common; they are inevitable. Content that a large body of people believe should be taken down is left up,[34] while content that many people believe should remain up is taken down.[35] Multiple content moderation employees may view content in entirely different lights, and it is next to impossible for content moderators to take context into account (in part because much of the context may not be available or evident to them and in part because the time required to investigate each situation fully makes it impossible to do cost effectively). Similarly, no technological solution can properly take context or intent into account—a computer cannot recognize things like satire or hyperbole, even at a level that would be obvious to any human reader.

A protocol-based system, however, moves much of the decision making *away from the center and gives it to the ends of the network*. Rather than relying on a single centralized platform, with all of the internal biases and incentives that that entails, anyone would be able to create their own set of rules—including which content do they not want to see and which content would they like to see promoted. Since most people would not wish to manually control all of their own preferences and levels, this could easily fall on any number of third parties—whether they be competing platforms, public interest organizations, or local communities. Those third parties could create whatever interfaces, with whatever rules, they wanted.

For example, those interested in civil liberties issues might subscribe to moderation filters or even add-on services released by the ACLU or the

EFF. Someone deeply involved in politics might choose a filter from their designated political party (while this obviously raises some concerns about an increase in "filter bubbles," there are reasons to believe the impact of such things would be limited, as we shall see).

Entirely new third parties could spring up focused entirely on providing a better experience. This need not just be around the content moderation filter, but around the entire user experience. Imagine a competing interface for Twitter that would be pre-set (and constantly updated) to moderate out content from trollish accounts, and to better promote more thoughtful, thought-provoking stories, rather than traditional clickbait hot takes. Or an interface could provide a better layout for conversations. Or for newsreading.

The key would be making sure that the "rules" are not only shareable but completely transparent and in the control of any end user. So, I might elect to use the EFF's openly available controls for Twitter, using an interface provided by a new non-profit, but then be able to tweak the settings if I prefer, say, more content about the EU. Or if I want to use the network mainly for reading news, I might use an interface provided by the New York Times. Or if I want to chat with friends, I could use a special interface designed for better communication among small groups of friends.

In such a world, we can let a million content moderation systems approach the same general corpus of content—each taking an entirely different approach—and see which ones work best. The centralized platforms are no longer the single-source arbiter of what is and what is not allowed. Rather, many, many different individuals and organizations would be able to tweak the system to their own levels of comfort and share them with others—and allow the competition to happen at the implementation layer, rather than at the underlying social network level.

This would not entirely prevent anyone from using the platform from speaking, but if the more popular interfaces and content moderation filters chose, entirely voluntarily, not to include them, the power and impact of their speech would be more limited. This, then, presents a more democratic approach, in which the marketplace of filters is enabled to compete. If people feel that one such interface or filter provider is not

doing a good job, they can move to another one or tweak the settings themselves.

Thus, we have less central control, less cause to claim "censorship," more competition, a wider range of approaches, and more control pushed to the end users—all while likely minimizing the reach and impact of content that many people find abusive. Indeed, the existence of a variety of different filter choices would likely change the reach of any individual proportionate to how problematic many consider that individual's speech to be.

As an example, there has been tremendous controversy over how platforms have handled the account of Alex Jones, the entertainer who runs InfoWars and has regularly supported various conspiracy theories. Users placed tremendous pressure on platforms to cut him off, and when they finally did, they faced corresponding pushback from his supporters claiming that they had only chosen to remove him from their platforms due to a bias against his politics.[36]

In a protocols-based system, those who have always believed that Jones was not an honest actor would likely have blocked him much earlier, while other interface providers, filter providers, and individuals could make a decision to intervene based on any particularly egregious act. While his strongest supporters would probably never cut him off, his overall reach would be limited. Thus, those who don't wish to be bothered with his nonsense need not deal with it; those who do wish to see it still have access to it.

The marketplace of the many different filters and interfaces (and the ability to customize your own) would enable much greater granularity. Conspiracy theorists and trolls would have more trouble being found on the "mainstream" filters but would not be completely silenced from those who wish to hear them. Rather than today's centralized system, where all voices are more or less equal (or completely banned), in a protocol-focused world the extremist views would simply be less likely to find mainstream appeal.

Protecting User Data and Privacy

A side benefit to this is that a protocol-based system would almost

certainly increase our privacy as well. Under such a system, social media-style systems would not need to collect and host all of your data. Instead, just as the filtering decisions could move to the end, so too might the data storage. While this could develop in many different ways, one fairly straightforward method is that end users would simply build their own "data stores" via apps that they control. Since it is unlikely that we'd move back to a world where most people would be storing data locally (especially since we increasingly do things from a number of devices, including computer, smartphone, and tablet), it could still make sense to host this data in the cloud, but the data could remain entirely under the control of the end user.

In such a world, you might use a dedicated data store company, which would host your data in the cloud as an encrypted blob that the data store provider would not have access to—but that you yourself could selectively enable access to for whatever purpose was necessary at any given moment. This data could act as your unique identity as well. Then, if you want to use the Twitter-like protocol, you could simply open up access to your databank for the Twitter-like protocol to access what is necessary. You would be able to set what it was allowed (and not allowed) to access, and you would also be able to see when and how it accessed your data and what it did with it. That means that you'd be able to cut off access at any time if anyone abused that access. In some cases, systems could be designed so that even as a service is accessing your data, it would be unable to collect specific data on you, only receiving aggregator or summary information in a hashed form, allowing an additional layer of privacy.

In this way, end users would still be able to make use of their own data for various social media tools, but rather than having that data locked up in opaque silos with no access, no transparency, and no control, the control would be moved entirely to the end users. The intermediaries are incentivized to be on their best behavior to avoid being cut off. The end user gets a better sense of how his or her data is actually used, and the ability to sign up for other services and even safely pass data from one entity to another (or multiple others) is improved, enabling powerful new features as well.

While there might be some fear that under such a system the various intermediaries would still be focused on sucking up all of your data, that need not be the case, for a few key reasons. First, given the ability to use the same protocol and switch to a different interface/filter provider, any provider that became too "greedy" for your data would run the risk of turning people off. Second, by separating the data store from the interface provider, the end user has much greater transparency. The idea is that you would store your data in a data store/cloud service in an encrypted format so that the hosting party would have no access to it. The interface provider would need to request access, and tools and services could be developed that would enable you (1) to determine what data platforms would be allowed to have access, for how long, and for what reasons and (2) to cut off that access if you were uncomfortable with how it was being used.

While it would be possible for an interface/filter operator to abuse its privileges to collect and keep your data, there are potential technical means around this as well, including designing the protocol such that it is expected to only pull your relevant data in close to real time from your data store. If it is not doing that and is accessing its own store of your data, warnings could be triggered that your data is being housed against your wishes.

Finally, as explained below in discussing the business model, there will be much stronger incentives for the interface providers to respect the privacy wishes of the end users, as their money is likely to be driven more directly by usage, rather than by monetizing the data. And upsetting your user base could lead them to flee, thereby harming the interface providers' own economic interests.

Enabling Greater Innovation

A protocol system, by its very nature, would likely lead to much more innovation in this space, in part by allowing anyone to create an interface for accessing this content. That level of competition would almost certainly lead to various attempts to innovate, improving all aspects of the service. Competing services could offer a better filter, a better interface, better or different features, and much more.

Right now, we have only inter-platform competition, which happens to some extent but is fairly limited. It is clear that the market can accept a few giants, so while Facebook, Twitter, YouTube, Instagram, and some others may compete here or there for user attention, there is less incentive] to improve their own services.

However, if anyone could present a new interface, or new features, or better moderation, then suddenly the competition within a specific protocol (previously a platform) could quickly become fierce. Various ideas might be tried and discarded, but the laboratory of the real world would likely show in short order how these services could innovate and provide more value much more quickly. Currently, many platforms offer up APIs that allow third parties to develop new interfaces, but the APIs are controlled by the central platforms—and they can change them on a whim. Indeed, Twitter has famously shifted its support for APIs and third party developers many, many times—but under a protocol system, the API would be open, with the expectation that anyone could build on it, and there wouldn't be a central company to cut a developer off.[37]

On top of that, it would likely create entirely new areas for innovation, including in ancillary services, such as parties that focus on providing better content moderation tools or the competing databanks discussed earlier, which would serve simply to host access to your encrypted data, without having to have access to it or perform any specific actions on it. Those services might compete on speed and uptime rather than additional features.

For example, in a world of open protocols and private data stores, it is possible that a thriving business could develop in the form of "agents" that interface between your data stores and various services, automating certain tasks and providing additional value. A simple version of this could be an agent focused on scanning various protocols and services for relevant news on a particular topic or company and then sending an alert to you once it finds anything.

Creating New Business Models

One of the main reasons that protocols from the early internet have faded in comparison to centralized platforms is the business model

issue. Having your own platform (if it catches on) has been a model that appears to print lots of money for the companies. However, building and maintaining a protocol has long been a struggle. Most of the work was usually done by volunteers, and protocols over time were known to atrophy without attention. For example, OpenSSL, a key security protocol that a very large percentage of the internet relied on, in 2014 was found to have a major security flaw known as Heartbleed. Around this time, it was noted that OpenSSL's support was almost entirely lacking. There was a loose group of volunteers and a single full-time person working on OpenSSL. The foundation that ran it historically had only received fairly modest grants.[38]

There are lots of stories like this. As mentioned earlier, Deja News couldn't build much of a business out of Usenet, so it was sold off to Google. Email was never seen as much of a moneymaker as a protocol, and it was usually included free with your ISP account. A few early companies tried to build web platforms around email, but two significant such examples were quickly bought by larger companies (Rocketmail by Yahoo, Hotmail by Microsoft) to fold into larger offerings.[39] Eventually Google launched Gmail, and it did a fair amount to pull email into its own platform, but it was rarely seen as a huge driver of revenue. Still, the success Google and Microsoft had had with Gmail and Outlook, respectively, show that large companies can build very successful services on top of open protocols. If Google really messed up Gmail or did problematic things with this service, it is not difficult for people to move to a different email system and to retain access to everyone they communicate with.

We've already discussed competition among the various interface and filter implementations to provide a better service, but there would also likely be competition for business models. There would probably be experiments with different types of business models involving both the data store services—which might charge for premium access and storage (as well as security)—much as services like Dropbox and Amazon Web Services do today. There might also be a variety of different business models formed around implementations and filters. There could be subscription offerings for premium services or features or alternative forms of payment as well.

And while there are—quite reasonable—concerns about the data surveillance setup of the current advertising market on today's social media platforms, there is reason to believe that a less data-intensive ad model might thrive in the world described here. Again, with the data and privacy levels in the hands of the end users, the more aggressive collection of all data would not be as viable or useful. Instead, it's possible a few different types of ad models might develop.

First, there could be an ad model based on much more limited data, with a greater focus on matching intentions or on pure brand advertising. For a glimpse of this possibility, look back at Google's original ad model, which didn't rely so much on knowing everything about you but rather on knowing the context of your internet searches at that specific moment. Or, we could move back to a world of more traditional brand advertising, where endemic advertisers would search out appropriate communities. For example, an automobile company would look to advertise within micro-communities on a platform who have a *stated* interest in cars.

Alternatively, given the amount of control end users would have over their data, there could develop a reverse auction type of business model, under which the end users themselves might be able to offer up their data in exchange for access or deals from certain advertisers. The key is that the end user—rather than the platform—would be in control.

Perhaps most interestingly, there are some potential new opportunities by which protocols might actually be much more sustainable. In the last few years, with the development of cryptocurrencies and tokens, it has become theoretically possible to build a protocol that uses a cryptocurrency or a token that has some value attached to it, with the value of those items growing in conjunction with usage.[40] A simple way of looking at this is that a token-based cryptocurrency is the equivalent of equity in a company—but rather than the value being tied to the financial success of the company, the value of a crypto token is tied to the value of the overall network.

Without getting too deep into the weeds on how these work, these forms of currency have a value all their own, and they are attached to the protocol they are supporting. As more people use the protocol, the currency or token *itself* increases in value. In many cases, the use of the

currency or token could be necessary to running the protocol itself—thus, as the protocol is more widely used, demand for the currency/token increases, while the supply remains constant or expands along a previously designed growth plan.

This creates incentives for more people to support and use the protocol to increase the value of the associated currency. There are attempts right now to build protocols where an organization in charge of the protocol retains some percentage of the currency while distributing the rest. In theory, under such a system, if it were to catch on, the appreciation in value of the tokens/currency could help fund the ongoing maintenance and operation of the protocol—effectively eliminating the historical problem of funding for open protocols that helped create the modern internet.

Similarly, there could be ways for the various implementers of interfaces or filters or agents to benefit from the increases in value of the tokens. Different models could result, but various implementations could be given a specific share of tokens, and as they help the network increase in usage, their own token value would increase as well. Indeed, token distribution could be tied to the number of users within a particular interface to create aligned incentives (albeit with some mechanism to avoid gaming the system with faked users). Or, as described above, the use of the tokens could be a necessary component of running the actual architecture of the systems, in the same manner that the Bitcoin currency is a key piece of how its open blockchain ledger functions.

In many ways, this setup better aligns the interests of the users of the service with the developers of the protocols and the interface designers. In a platform-based system, the incentives are either to charge users directly (putting the interests of the platform and the user somewhat at odds) or to collect more of their data to advertise to them. Theoretically, "good" advertising might be seen as valuable to end users, but in most cases, end users feel that the interests of the platform and the users tends to be misaligned when the platform is collecting so much data with the intention of targeting ads to them.

Under a tokenized system, however, the key driving factor is in getting more usage to increase the value of the tokens. This could, obviously, create other incentive challenges—there are already concerns about plat-

forms sucking up too much time, and any service faces challenges when it grows too big—but again, a protocol would encourage competition to provide better user interfaces, better features and better moderation, thereby minimizing this challenge. Indeed, an interface might compete by providing a more limited experience and promote itself for its ability to limit information overload.

Still, the ability to align the incentives of the network itself with a financial benefit creates a rather unique opportunity that many are now exploring.

WHAT MIGHT NOT WORK

NONE OF THIS IS TO SAY that a protocols-based system would solve all ills definitively. Much of what is suggested above is speculative—and, indeed, we've already seen historically that platforms overtook protocols, while protocols had limited ability to thrive.

Complexity Kills

It is entirely possible that any protocols-based system will tend to be too complicated and too cumbersome to attract a large enough userbase. Users don't want to fiddle with tons of settings or different apps to get things to work. They just want to find out what the service is and be able to use it without much difficulty. Platforms have historically been quite good at focusing on the user experience aspect, especially around onboarding new users.[41]

One would hope, if we were to attempt a new protocols-based regime, that it could and would take lessons from the success of platforms these days and build on them. Similarly, the intra-protocol competition at the service level might create greater incentives for creating a better user

experience—and the same would be true of the value of an associated cryptocurrency whose value is literally tied to the creation of a better user experience. Indeed, providing the easiest and most user-friendly interface to access the protocol would likely be a key area of competition.

Finally, one of the reasons why platforms won out historically is that having everything controlled by a single entity also leads to some clear performance boost. In a world of protocols with separate data stores/interfaces, you would be much more reliant on multiple companies connecting together without delay. The internet giants like Google, Facebook, and Amazon have really perfected having their own systems work together seamlessly, and introducing multiple third parties into the mix would bring greater risk. However, there have been widespread technological improvements in this area (and, indeed, the large platform companies have open-sourced some of their own technologies that enabled this). On top of that, broadband speeds have increased and should continue to do so, possibly minimizing this possible technical hurdle.

Existing Platforms Are Too Big and Will Never Change

Another potential stumbling block is that existing platforms—Facebook, YouTube, Twitter, Reddit, and the like—are already so large and so entrenched that it would be nearly impossible to unseat them with a protocols-based approach. This criticism presumes that the only way to achieve this is for a brand-new system to come about that relies on protocols. That could work, but the platforms themselves might consider using protocols as well.

The response many will have to the idea that the platforms could do this themselves is to ask why they would do this, since it would inevitably mean getting rid of the monopolistic control they currently enjoy over the information in their system and allowing that data to return to the control of the end user and be used on competing services using the same protocol. However, there are a few reasons to think that some platforms might actually be willing to accept this tradeoff.

First off, as pressure on these platforms increases, they are increasingly going to need to acknowledge that what they are currently doing

does not work and is unlikely to ever work. The current mode of operation is only going to lead to ever more pressure to "solve" what appear to be unsolvable problems. At some point, moving to a protocols system may be a way for the existing platforms to relieve themselves of the impossible burden of being the steward of what every person on their platform is doing.

Second, continuing with what they are doing is going to be increasingly costly. Already Facebook recently promised to hire another 10,000 moderators; YouTube has also promised to hire "thousands" of moderators.[42] Hiring all those people is going to be an increasing cost on these companies as well. Switching to a protocols-based system would move the moderation element out to the ends of the networks or to competing third parties, taking that expense off the books for the large platforms.

Third, the existing platforms may explore the use of protocols as an effective way of competing against *other large internet platforms* in areas where they have much less ability to compete. For example, Google has tried and given up on multiple attempts at building a Facebook-style social network.[43] However, if it continues to believe that there should be an alternative social network to Facebook, it may recognize the appeal of offering an open protocols-based system. In effect, recognizing that it would be unlikely to be able to build its own proprietary solution would make offering up an open protocol system an appealing alternative, if only to cut away at Facebook's position.

Finally, if the token/cryptocurrency approach is shown to work as a method for supporting a successful protocol, it may even be more valuable to build these services as protocols, rather than as centralized, controlled platforms.

This Will Worsen the Filter Bubble Issue

Some have argued that this approach would actually make some of the problems regarding abusive content online even worse. The argument is that allowing abusive individuals—whether mere trolls or horrifying neo-Nazis—to have any ability to speak their minds is going to be a problem. And to take it a step further, they would argue that by allowing for competing services, you'd end up with cesspool areas of the internet,

where the worst of the worst would continue to gather unimpeded.

While I am sympathetic to this possibility, this does not seem to be inevitable by any stretch of the imagination. One point against this complaint is that we already have those people infesting the various social networks, and nothing so far has been successful in getting rid of them. But the larger point is that this would likely quarantine them to some extent, as their content would be less likely to get into the most widely used implementations and services on the protocol. That is, while they would be able to be vile in their own dark corners, their ability to infect the rest of the internet and (importantly) to seek out and recruit others would be severely limited.

To some extent, we have already seen this in action. When forced to congregate in their own corners of the internet after being expelled from sites like Facebook and Twitter, alternative services that cater solely to those users have not been particularly successful in scaling up or growing over time. There will always be some people with crazy ideas—but allowing them their own little space in which to be crazy might better protect the wider internet, rather than constantly having to kick them off every other platform.

Dealing with More Objectively Problematic Content

A key assumption in much of this is that much of the "objectionable" content creating the headaches here are in a broad "gray" spectrum, rather than "black and white." However, there is some content—often content that violates various laws—that is much clearer and not in the middle of the spectrum. There are legitimate reasons to raise concerns about how this setup might allow communities to form around things like child porn, revenge porn, stalking, doxing, or other criminal activities.

Of course, the reality is that these kinds of communities are already forming—often on the dark web—and the way they are dealt with today is mostly via law enforcement (and sometimes with investigative reporting). It seems quite likely that the same would be true under this setup as well. There is little reason to think that in a protocol-focused world, this problem would be all that different than what currently exists.

Also, with an Open protocols system, there actually would be greater transparency, and some (such as civil society groups who monitor hate groups or law enforcement bodies) would even be able to build and deploy agents that monitor those spaces and would be able to set off notifications of particularly egregious commentary that requires more direct scrutiny. Someone who is being stalked, rather than having to track the stalker directly, might employ a digital agent to scan the wider set of protocols to determine if there is any content that suggests a concern and then directly alert the police or other relevant contacts.

EXAMPLE IN ACTION/HOW IT WOULD LOOK IN PRACTICE

AS DESCRIBED ABOVE, there are many ways this might play out. Existing services might find that the burdens of being a centralized platform are becoming too costly and so seek out an alternative model—and a tokenized/cryptocurrency approach might even make that fiscally feasible.

Alternatively, new protocols might be created to enable this. There are already a number of attempts at various levels. Services like IPFS (InterPlanetary File System) and its related offering Filecoin are already laying the groundwork and infrastructure for a distributed set of services built on its protocol and currency.[44] The inventor of the World Wide Web itself, Tim Berners-Lee, has been working on a system called Solid, now housed at his new company Inrupt, that would help enable a more distributed internet.[45] Other projects such as Indieweb have been bringing people together to build many of the pieces that could contribute to a future world of protocols instead of platforms.[46]

In either case, if a protocol were set forth and began to pick up traction, we'd expect to see a few key things: multiple implementations/services on the same protocol, providing users a choice of which service to use, rather than limiting them to just one. We'd also likely start to see the rise of a new line of businesses involving secure data storage/data stores, as users would move away from making their data freely available to platforms and be more in control. It is likely that other new services and opportunities would spring up as a result of this as well, especially as there would be increasing competition to build a better set of services for users.

CONCLUSION

Over the last half-century of networked computing, a pendulum has been swinging between client-side and server-side computing. We went from mainframes and dumb terminals to powerful desktop computers to web apps and the cloud. Perhaps we will start to see a similar pendulum in this arena as well. We've gone from a world in which protocols dominated to one in which centralized platforms controlled all. Moving us back toward a world where protocols are dominant over platforms could be of tremendous benefit to free speech and innovation online.

Such a move has the potential to return us to the early promise of the web: to create a place where like-minded people can connect on various topics around the globe and anyone can discover useful information on a variety of different subjects without it being polluted by abuse and disinformation. Simultaneously, it could enable greater competition and innovation on the internet, while also giving end users more control over their own data and preventing giant corporations from having too much data on any particular user.

Moving to protocols, not platforms, is an approach for free speech in

the 21st century. Rather than relying on a "marketplace of ideas" within an individual platform—which can be hijacked by those with malicious intent—protocols could lead to a marketplace of ideals, where competition occurs to provide better services that minimize the impact of those with malicious intent, without cutting off their ability to speak entirely.

It would represent a radical change, but one that should be looked at seriously.

NOTES

1 Zachary Laub, *Hate Speech on Social Media: Global Comparisons*, Council on Foreign Rel. (Jun. 7, 2019), https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons.

2 Tony Romm, *Republicans Accused Facebook, Google and Twitter of Bias. Democrats Called the Hearing 'Dumb.'*, Wash. Post (Jul. 17, 2018), https://www.washingtonpost.com/technology/2018/07/17/republicans-accused-facebook-google-twitter-bias-democrats-called-hearing-dumb/?utm_term=.895b344999816.

3 Matt Laslo, *A Conversation with Mark Warner: Russia, Facebook and the Trump Campaign*, Radio IQ|WVTF Music (Apr. 6, 2018), https://www.wvtf.org/post/conversation-mark-warner-russia-facebook-and-trump-campaign#stream/0 (statement of Sen. Mark Warner: "I first called out Facebook and some of the social media platforms in December of 2016. For the first six months, the companies just kind of blew off these allegations, but these proved to be true; that Russia used their social media platforms with fake accounts to spread false information, they paid for political advertising on their platforms. Facebook says those tactics are no longer allowed—that they've kicked this firm off their site, but I think they've got a lot of explaining to do.").

4 Nicholas Confessore & Matthew Rosenberg, *Facebook Fallout Ruptures Democrats' Longtime Alliance with Silicon Valley*, N.Y. Times (Nov. 17, 2018), https://www.nytimes.com/2018/11/17/technology/facebook-democrats-congress.html ("[Sen. John] Tester, the departing chief of the Senate Democrats' campaign arm, looked at social media companies like Facebook and saw propaganda platforms that could cost his party the 2018 elections, according to two congressional aides. If Russian agents mounted a disinformation campaign like the one that had just helped elect Mr. Trump, he told Mr. Schumer, 'we will lose every seat.'").

5 Julia Carrie Wong, *#BreakUpBigTech: Elizabeth Warren Says Facebook Just Proved Her Point*, The Guardian (Mar. 11, 2019), https://www.theguardian.com/us-news/2019/mar/11/elizabeth-warren-facebook-ads-break-up-big-tech (statement of Sen. Elizabeth Warren) ("Curious why I think FB has too much power? … Let's start with their ability to shut down a debate over whether FB has too much power. Thanks for restoring my posts. But I want a social media marketplace that isn't dominated by a single censor. #BreakUpBigTech.").

6 Jessica Guynn, *Ted Cruz Threatens to Regulate Facebook, Google and Twitter Over Charges of Anti-Conservative Bias*, USA Today (Apr. 10, 2019), https://www.usatoday.com/story/news/2019/04/10/ted-cruz-threatens-regulate-facebook-twitter-over-alleged-bias/3423095002/ (statement of Sen. Ted Cruz) ("What makes the threat of political censorship so problematic is the lack of transparency, the invisibility, the ability for a handful of giant tech companies to decide if a particular speaker is disfavored.").

7 Press Release, Louie Gohmert, U.S. Congressman, *Gohmert Introduces Bill That Removes Liability Protections for Social Media Companies That Use Algorithms to Hide, Promote, or Filter User Content* (Dec. 20, 2018), https://gohmert.house.gov/news/documentsingle.aspx?DocumentID=398676 ("Employees from some of these companies have communicated their disgust for conservatives and discussed ways to use social media platforms and algorithms to silence and prevent income to conservatives.").

8 April Glaser, *Want a Terrible Job? Facebook and Google May Be Hiring*, Slate (Jan. 18, 2018), https://slate.com/technology/2018/01/facebook-and-google-are-building-an-army-of-content-moderators-for-2018.html (explaining that major platforms have hired or have announced plans to hire thousands, in some cases more than ten thousand, new content moderators).

9 Tom Simonite, *AI Has Started Cleaning Up Facebook, But Can It Finish?*, Wired (Dec. 18, 2018), https://www.wired.com/story/ai-has-started-cleaning-facebook-can-it-finish/.

10 Gohmert Press Release, *supra* note 7 ("Social media companies enjoy special legal protections under Section 230 of the Communications Act

of 1934, protections not shared by other media. Instead of acting like the neutral platforms they claim to be in order to obtain their immunity, these companies have turned Section 230 into a license to potentially defraud and defame with impunity … Since there still appears to be no sincere effort to stop this disconcerting behavior, it is time for social media companies to be liable for any biased and unethical impropriety of their employees as any other media company. If these companies want to continue to act like a biased medium and publish their own agendas to the detriment of others, they need to be held accountable."); Eric Johnson, *Silicon Valley's Self-Regulating Days "Probably Should Be" Over, Nancy Pelosi Says*, Vox (Apr. 11, 2019), https://www.recode.net/podcasts/2019/4/11/18306834/nancy-pelosi-speaker-house-tech-regulation-antitrust-230-immunity-kara-swisher-decode-podcast (statement of House Speaker Nancy Pelosi) ("230 is a gift to them, and I don't think they are treating it with the respect that they should … . And so I think that that could be a question mark and in jeopardy … . For the privilege of 230, there has to be a bigger sense of responsibility on it, and it is not out of the question that that could be removed.").

11 Robert Burnson, *Twitter Beats Censorship Lawsuit by Banned White Nationalist*, Bloomberg (Aug. 23, 2018), https://www.bloomberg.com/news/articles/2018-08-24/twitter-beats-censorship-lawsuit-by-banned-white-advocate (self-proclaimed "white advocate" Jared Taylor argued that it was a violation of his rights to be removed from Twitter, but a California state appeals court rejected that argument).

12 For example, Google's Gmail service is based on open email protocols like SMTP and IMAP, but with additional features built on top of it. Facebook uses the Signal Protocol to handle end-to-end encryption for its WhatsApp and Facebook Messenger services.

13 Alex Hern, *How Social Media Filter Bubbles and Algorithms Influence the Election*, The Guardian (May 22, 2017), https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles.

14 *Everybody Wants to Rule the World*, The Economist (Nov. 27, 2014), https://www.economist.com/briefing/2014/11/27/everybody-wants-to-rule-the-world.

15 *About Usenet: Information About Usenet and Usenet.nl*, Usenet.il, https://en.usenet.nl/usenet/; *The Conversation Starts Here*, Reddit, https://www.redditinc.com.

16 Michelle Delio, *Google Buys Deja Archive*, Wired (Feb. 12, 2001), https://www.wired.com/2001/02/google-buys-deja-archive/.

17 *Eternal September*, Tv Tropes, https://tvtropes.org/pmwiki/pmwiki.php/Main/EternalSeptember ("Then, in 1993, AOL opened up the then-dominant forum of the 'net, Usenet, to every customer, and Usenet was overrun. The social structure that had worked fine to incorporate a relative handful of newcomers was ineffective in a world where the newcomers vastly outnumbered the old guard. Worse, for every newbie that could be civilized or driven off, more and more took their place immediately. This is the Eternal September, the age the [i]nternet now lives in; most of the old guard are gone, vanished, or formed more minor net societies within the larger [i]nternet as a whole.").

18 *Kill File*, Catb.org, http://catb.org/jargon/html/K/kill-file.html ("Per-user file(s) used by some Usenet reading programs (originally Larry Wall's rn(1)) to discard summarily (without presenting for reading) articles matching some particularly uninteresting (or unwanted) patterns of subject, author, or other header lines. Thus, to add a person (or subject) to one's kill file is to arrange for that person to be ignored by one's newsreader in future.").

19 *Moderated Newsgroups*, Big-8, https://archive.is/20120804234307/http:/www.big-8.org/wiki/Moderated_Newsgroups%23Who_can_force_the_moderators_to_obey_the_group_charter.3F#Who_can_force_the_moderators_to_obey_the_group_charter.3F.

20 Mike Isaac & Cecilia Kang, *Facebook Expects to Be Fined Up to $5 Billion by F.T.C. over Privacy Issues*, N.Y. Times (Apr. 24, 2019), https://www.nytimes.com/2019/04/24/technology/facebook-ftc-fine-privacy.html.

21 Emily Bell, *Facebook's Moderation Is of Public Interest. It Should Be Public Knowledge*, Colum. Journalism Rev. (May 23, 2017), https://www.cjr.org/tow_center/facebook-moderation-guardian.php.

22 Veronica Rocha, Brian Ries & Amanda Wills, *Mark Zuckerberg Testifies Before Congress*, CNN (Apr. 11, 2018), https://www.cnn.com/politics/live-news/mark-zuckerberg-testifies-congress/index.html.

23 Romm, *supra* note 2.

24 *Email Protocols – POP3, SMTP and IMAP Tutorial*, SiteGround, https://www.siteground.com/tutorials/email/protocols-pop3-smtp-imap/ (providing a description of protocols).

25 *Comparison of Email Clients*, Wikipedia, https://en.wikipedia.org/wiki/Comparison_of_email_clients (providing a long list of email clients).

26 Bill Slawski, *Early Yahoo Acquisitions (the 1990s)*, SEO by the Sea (Jan. 3, 2006), http://www.seobythesea.com/2006/01/early-yahoo-acquisitions-the-1990s/; *Google + E-mail = Gmail*, CNN Money (Apr. 1, 2004), https://money.cnn.com/2004/04/01/technology/google_email/.

27 *Check Emails from Other Accounts*, Gmail Help, https://support.google.com/mail/answer/21289?co=GENIE.Platform%3DDesktop&hl=en (last visited Dec. 31, 2019) (offering the Gmail fetcher setup as a way to use a non-Gmail address with the Gmail interface).

28 Brady Gavin, *The Best Chrome Extensions for Making Gmail Better*, How-To Geek (Feb. 27, 2019), https://www.howtogeek.com/402035/the-best-chrome-extensions-for-making-gmail-better/ (providing an example of the number of add-ons for email systems today that will work across multiple email implementations).

29 Rahul Biswal, *Top 10 Best Free Email Service Providers*, Ecloudbuzz (Dec. 31, 2018), https://www.ecloudbuzz.com/best-free-email-service-providers/ (providing lists of popular email services that show a range of big, recognizable companies like Google, Microsoft, AOL, and Yahoo along with startups).

30 Christina Warren, *Twitter's API Update Cuts off Oxygen to Third-Party Clients*, Mashable (Aug. 16, 2012), https://mashable.com/2012/08/16/twitter-api-big-changes/.

31 Amy Gesenhues, *Facebook Cuts off Access to API Platform for 'Hundreds of Thousands' of Inactive Apps*, Marketing Land (Aug. 1, 2018), https://marketingland.com/facebook-cuts-off-access-to-api-platform-for-hundreds-of-thousands-of-inactive-apps-245265.

32 Boomerang For Gmail, https://www.boomeranggmail.com (last visited Dec. 31, 2019).

33 Nick Hopkins, *Revealed: Facebook's Internal Rulebook on Sex, Terrorism and Violence*, The Guardian (May 21, 2017), https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence.

34 Parker Molloy, *By Not Banning Alex Jones, Twitter is Making a Political Choice*, The Verge (Aug. 8, 2018), https://www.theverge.com/2018/8/8/17662140/twitter-infowars-alex-jones-apple-facebook-spotify-pinterest-ban (explaining the criticism Twitter received for waiting long after most other internet platforms in removing the account of conspiracy theorist Alex Jones).

35 Sam Levin, Julia Carrie Wong & Luke Harding, *Facebook Backs Down From 'Napalm Girl' Censorship and Reinstates Photo*, The Guardian (Sep. 9, 2016), https://www.theguardian.com/technology/2016/sep/09/facebook-reinstates-napalm-girl-photo.

36 Eli Rosenberg, *Facebook Wants to Cut Down on Misinformation. So Why Isn't It Doing Anything About Infowars?*, Wash. Post (Jul. 14, 2018), https://www.washingtonpost.com/news/the-intersect/wp/2018/07/14/facebook-wants-to-cut-down-on-misinformation-so-why-isnt-it-doing-anything-about-infowars/?utm_term=.eacf34e87542.

37 *About Twitter's APIs*, Twitter Help Center, https://help.twitter.com/en/rules-and-policies/twitter-api.

38 Jon Brodkin, *Tech Giants, Chastened by Heartbleed, Finally Agree to Fund OpenSSL*, Ars Technica (Apr. 24, 2014), https://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-fund-openssl/ ("The open source cryptographic

software library secures hundreds of thousands of Web servers and many products sold by multi-billion-dollar companies, but it operates on a shoestring budget. OpenSSL Software Foundation President Steve Marquess wrote in a blog post last week that OpenSSL typically receives about $2,000 in donations a year and has just one employee who works full time on the open source code.").

39 Samuel Gibbs, *How Did Email Grow From Messages Between Academics to a Global Epidemic?*, The Guardian (Mar. 7, 2016), https://www.theguardian.com/technology/2016/mar/07/email-ray-tomlinson-history.

40 Tom Simonite, *The Decentralized Internet Is Here, with Some Glitches*, Wired (Mar. 5, 2018), https://www.wired.com/story/the-decentralized-internet-is-here-with-some-glitches/.

41 Yoav Vilner, *Cryptocurrency Exchanges Are Getting Better in User Experience and Liquidity*, Forbes (Jul. 14, 2018), https://www.forbes.com/sites/yoavvilner/2018/07/14/cryptocurrency-exchanges-are-getting-better-in-user-experience-and-liquidity/#20d5744b37f3.

42 Anita Balakrishnan, *Facebook Pledges to Double Its 10,000-person Safety and Security Staff by End of 2018*, CNBC (Oct. 31, 2017), https://www.cnbc.com/2017/10/31/facebook-senate-testimony-doubling-security-group-to-20000-in-2018.html.

43 Claire Cain Miller, *Another Try by Google to Take on Facebook*, N.Y. Times (Jun. 28, 2011), https://www.nytimes.com/2011/06/29/technology/29google.html.

44 *Go-Filecoin 0.2.2 Is Released*, Filecoin (May 17, 2019), https://filecoin.io/blog/go-filecoin-0.2.2-release/.

45 *The Evolution of Solid*, Solid, https://solid.inrupt.com/about (last visited Dec. 31, 2019).

46 *What is the IndieWeb?*, IndieWebCamp, https://indieweb.org/ (last visited Dec. 31, 2019).

About the Author

MIKE MASNICK is the founder and CEO of Floor64 and editor of the Techdirt blog. He is also the founder and CEO of the Silicon Valley-based Copia Institute, a think tank exploring innovative approaches to tech policy.

About the Knight First Amendment Institute

The Knight First Amendment Institute at Columbia University defends the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. Its aim is to promote a system of free expression that is open and inclusive, that broadens and elevates public discourse, and that fosters creativity, accountability, and effective self-government.

knightcolumbia.org

Design: Point Five
Illustration: © Sara Wong

KNIGHT
FIRST AMENDMENT
INSTITUTE

at Columbia University