



# Improving Social Media with Middleware

By  
ETHAN ZUCKERMAN   
and  
ISAAC BRICKMAN 

Middleware is software that can give users increased control over their social media experience, allowing them to protect their privacy, customize their recommendations, and understand the spread and impact of content they create. We believe middleware could complement policy efforts and reforms made by social media platforms to improve user experiences on social media, while avoiding freedom of expression questions that plague the regulation of online platforms. We describe and examine middleware as it exists in the world, demonstrating that even while middleware is a viable solution to some contemporary problems attendant to social media, there are still open questions about who middleware helps and who it harms. We suggest Federal Trade Commission (FTC) regulation of middleware and show that U.S. Code 47 section 230(b) anticipated categories of middleware that would be protective of users' control over their online experiences.

*Keywords:* middleware; social media; privacy; algorithms; internet policy

In less than 20 years, social media platforms have profoundly transformed the public sphere by creating new spaces to report news (Hendrickx and Opgenhaffen 2024), organize protests and political movements (Tufekci 2017; Freelon et al. 2016), discuss and deliberate political and social issues, and engage in political behavior through the dissemination of information (Zuckerman 2014). These changes

*Ethan Zuckerman is an associate professor of public policy, information, and communication at the University of Massachusetts Amherst. He is the author of Rewire (2013), Mistrust (2021), and the forthcoming A Field Guide to Social Media with Chand Rajendra-Nicolucci.*

*Isaac Brickman recently received a bachelor of arts degree from the University of Massachusetts Amherst. He plans to attend law school and aims to work at the intersection of law and technology. He is the host of the podcast Office Hours.*

Correspondence: ethanz@umass.edu

DOI: 10.1177/00027162251382700

to public discourse have been far from smooth. Numerous concerns about platform power and influence have surfaced, including the emergence of surveillance capitalism (Zuboff 2019), political polarization, filter bubbles (Pariser 2011), echo chambers (Sunstein 2017), and mis/disinformation (Wardle and Derakhshan 2017; Starbird et al. 2023; DiResta 2018). The current president and his former senior advisor Elon Musk are examples of powerful political figures who have been able to exert substantial control over social media platforms, raising concerns about their direct political influence over platform content. We have already seen this play out with Musk using his X account to amplify pro–Alternative for Germany voices, which led to increased social media engagement for the German far-right extremist party (Scott and Marsh 2025). At the same time, critics of platform power on the right have argued that attempts to control the spread of misinformation have constituted the censorship of conservative voices online (Mosleh et al. 2024).

These problems can make government platform oversight seem like an appealing solution. Yet platform oversight presents a conundrum for would-be regulators. Social media platforms host the speech of billions of actors, not all of whom are operating in good faith. For example, removing commercial spam from platforms clearly imposes limits on the speech of spammers, but failing to do so could easily result in platforms that are virtually unusable.

Responding to concerns that platforms were removing content aligned with right-wing points of view, the states of Florida and Texas both passed laws seeking to prevent social media platforms from removing posts that were based on ideology (Social Media Platforms 2021). The Supreme Court’s review of *Moody v. NetChoice LLC* (2024) unanimously remanded the case to lower courts. The decision asserted that platforms have the right to moderate most content, such as that delivered through the Facebook News Feed. Yet, because platforms have varied affordances and functionalities, the laws were not struck down.<sup>1</sup> It is likely that legislative actions taken to combat toxic speech on social media platforms could face similarly nuanced First Amendment obstacles. However, in the age of Trump, such legislation may be unnecessary, as major platforms such as Meta seem to be taking a permissive stance on content moderation (e.g., Mark Zuckerberg’s recent apology for censoring COVID-19 misinformation [Associated Press 2024]).

At the same time, ample evidence supports the contention that platforms often moderate less than they could, and possibly less than they should. Nicole Gill, the executive director and cofounder of Accountable Tech, articulated this point of view in commenting on the *NetChoice* decision:

Today’s unanimous opinion ensures platforms can enforce their community and safety standards during a critical election year, but make no mistake: this is not an excuse for platforms to continue to shrug off their role in the desecration of democracy and proliferation of a myriad of societal harms. These cases are part of a larger agenda by NetChoice and the tech industry to overturn tech regulation policies nationwide in an effort to protect Big Tech’s profit and influence. It is essential that we do not allow this decision to absolve Big Tech companies of their responsibility to protect our kids, defend democracy, and address threats to public safety (Gill 2024).

Internal documents leaked by Facebook employee Frances Haugen that suggest an unwillingness to act on pressing issues (e.g., Instagram's effects on body image) substantiate Gill's claim (Mac and Kang 2021). The fact that platforms have taken action to control the spread of disinformation at sensitive moments—as in the wake of the January 6 riots at the U.S. Capitol—raises the question of why social media platforms do not operate in such a manner all the time.

Platform oversight is complicated by the fact that platforms have different utility—and different pitfalls—for different users. A platform that exposes one teenager to content harmful to her body image just might connect another to an LGBTQ+ support system absent in their immediate community. Many platform governance solutions are likely to benefit one set of users at the expense of another: A time limit on social media designed to help users struggling with overuse might harm others who find community and support online. Effecting platform-wide solutions is inherently a problematic undertaking.

For example, the proposed Kids Online Safety Act (2023) legislation is designed mainly to make platforms provide a “duty of care” to minors when designing or implementing potentially harmful features, give tools for parents to supervise a child's use of the platform, and limit features that might increase the amount of time minors spend on it (J 2024). These are reasonable aspirations. But as danah boyd (2024) has observed in an analysis of the proposed legislation, legitimate attempts to protect children from online harm—by giving parents more control over social media—are likely to harm youth whose parents are abusive and for whom the internet might provide a safe space and outlet. (Moreover, parental abuse of children is sufficiently widespread that this concern needs significant consideration.) She also argues that technological solutionism is not the quick fix some may think: “The solution is not ‘make tech fix society’” (boyd 2024).

“The intervention we need to an ecological problem is an ecological one” (boyd 2024). The world is complicated, and using technology as a scapegoat for the mental health crisis—taking away children's social lives and First Amendment rights in the process—might not be the answer.

What does a nuanced, ecosystem-wide approach to platform oversight look like? We know that leaving governance up to platforms abdicates our collective responsibility for online speech. And if legislative efforts run afoul of First Amendment obstacles and the possibility of overbroad legislation, what alternatives remain?

We believe that middleware may be part of that alternative. It offers a solution that is complementary to both platform reform and government regulation. Middleware allows individual users to add features and capabilities to social media platforms to increase utility, protect privacy, or reduce known harms. Using middleware is a voluntary action taken by a user to shape the platform experience to better meet her needs. In most cases, a user's use of middleware does not positively or negatively impact other platform users. However, as we will examine, some middleware products can create privacy concerns and negative financial implications for platforms, advertisers, and influencers.

Notably, middleware is a market-based solution in a sector where social media platforms often have concentrated market power and reach. Hirschman's (1970)

distinction between the consumer's choices—"exit" and "voice"—can seem meaningless in the context of a network like Facebook. You can exit, and you can even retain the content you've posted to the platform. But you cannot simply move to another platform and replicate your experience on Facebook unless all your friends leave with you. Voice is similarly problematic. As the famous internet maxim goes, "If you're not paying for something, you're not the customer, but the product being sold."<sup>2</sup> As such, demanding changes to a platform that a user does not pay to use seldom leads to significant change.

But middleware offers users a choice: If you want to use a particular feature, you can choose to install an appropriate piece of software. If that middleware software is difficult to write or maintain, its authors will likely charge for their product. If that feature is sufficiently desirable, a critical mass of users could ensure there is a viable business in providing that functionality. In markets that appear concentrated and monopolistic, middleware is a solution that could leverage competitive dynamics and produce features unlikely to be offered by the platforms on their own.

Middleware also creates a secondary effect: A piece of middleware demonstrates that a social media system could operate in a different way, and the widespread adoption of a middleware product could offer a reliable signal to social media platforms of how at least *some* users want their technologies to operate.

Anecdotally, we may have seen evidence of the signaling function for middleware in an early deployment of Gobo, the social media aggregator our lab has developed over the past eight years. An early design of Gobo, released by our lab at the Massachusetts Institute of Technology, included information on why a particular post was present in your feed. Within a month of our release of that tool and code to the public, Facebook implemented a similar feature on its site. It is very unlikely that Facebook "copied" the feature from Gobo. It is more likely that an internal debate had existed about implementing the feature and that then seeing the feature "in the wild" might have swayed the debate.

In the absence of platforms' voluntary creation of prosocial infrastructures, and given a constricted U.S. policymaking environment, we believe middleware can serve as an alternative. These products can create an architecture that limits negative experiences, encourages positive behavior and, in the process, pressures platforms to adopt the positive features that middleware offers. The best of these features are based around algorithmic autonomy, privacy, and safety.

Before describing middleware as it currently exists in the world, it is worth noting how we define our audience. We are writing for at least three. One is policymakers: We want them to understand that there are options for fixing social media beyond legislating procedural changes to platforms. A second is developers: We hope to encourage them to improve platforms by giving them language to talk about what they're doing and by advocating for a legal environment that makes it safer to develop tools. The third is users: We want those who are dissatisfied with social media as it stands to know that middleware offers an alternative to exiting platforms or protesting against them.

## Middleware in the World

Stanford Professor Francis Fukuyama and colleagues (2021) made a compelling argument for middleware as a superior intervention to other solutions to improved platform governance, suggesting that the ability to choose among implementations made middleware more flexible than other interventions. They offer the example of a fact-checking service implemented in middleware, not by a platform as a whole: Each user could choose the provider they viewed as most reliable to filter out less factual content. The authors acknowledge that, at the time they were writing, middleware was at least as much a theory as an active practice: “We explicitly acknowledge that we offer here only a conceptual outline of a middleware approach and that much thinking remains to be done” (Fukuyama et al. 2021, 7).

Our lab has been actively involved in producing middleware, notably the Gobo.social aggregator and filtering architecture (Lane 2022; Bhargava et al. 2019), and in mapping the space of existing middleware (Brickman 2025). The results of our efforts to catalog the space make clear that middleware not only exists but has an expanding user base. By examining the benefits and challenges of existing middleware systems, we can identify which problems middleware is best suited to address.

Fukuyama et al. (2021, 5) define middleware as “software products that can be appended to the major internet platforms,” usually using an application programming interface (API), to “allow consumers to shape their feeds and influence the algorithms that those dominant platforms currently employ.” We agree that this is a key use of middleware; indeed, our Gobo.social platform exists as a framework for tools that shape user feeds (Lane 2022; Rajendra-Nicolucci et al. 2023). However, by examining middleware in the world, we have come to believe these products’ potential reaches beyond algorithmic ranking. In surveying the broader middleware space, we see at least three other ways middleware is being used: to strengthen user privacy on social media platforms, to provide analytics and performance information that is otherwise unavailable, and to improve user experience. It is worth noting that every instance of middleware use provides users with more control over their social media experience and offers features not provided by a platform. Increased control is foundational to the current and potential viability of middleware.

A taxonomy published by our lab offers definitions of subcategories of middleware and examples of each type of product currently in the market. We offer an overview of each of these categories and examples to demonstrate how middleware currently in use operates.

### *Privacy-strengthening tools*

In 2018, Tracy Chou released Block Party (Morris 2024), a commercial middleware application that added a key feature to Twitter. As a female software developer and entrepreneur who organized projects to document gender

imbalances in software development (Chou 2013), Chou routinely experienced a level of harassment on Twitter (Perez 2024) that might be unusual for most platform users but is sadly common for women activists online. Twitter allowed Chou to block an individual who sent her a death threat but did not provide an easy way to block the users who had liked or retweeted that threat. Block Party was released as a piece of middleware that interoperated with Twitter's API to provide advanced blocking features: mass blocking of people who had liked or amplified an offensive tweet and access to blacklists of known harassers.

While Twitter could have incorporated the mass-blocking features Block Party offered, it did the opposite. When Elon Musk acquired the company and transformed it into X, he raised prices sharply for API access, forcing many research projects and API-dependent start-ups to close. Block Party no longer provides the mass-blocking functions it was designed around, but it has pivoted to a privacy-enhancement model in which the software scans user settings on different social media platforms and recommends setting changes to make platform use more secure (Bond 2021).

Like Block Party, Redact aims to increase privacy across multiple platforms. It focuses on deleting user-generated content, a task that could be onerous if a user is an active poster on a site like Reddit. The motivations for those using Redact are perhaps less laudable than for those using Block Party; the company's founder, Dan Saltman, cites an athlete selected in a professional sports draft who wants to clean up his social media presence before becoming the face of a franchise or a brand (Zuckerman 2025). However, the functionality provided by Redact addresses a legitimate user need that platforms have little or no incentive to provide, unless forced by regulation.

### *Analytics tools*

A major question for social media users is who is seeing their posts and how they are reacting to them. While most platforms provide basic counts of interactions (e.g., "likes" or message forwards), many social media creators want more in-depth information. We see two types of middleware that act as social media analytics tools: commercial and personal. Commercial analytics tools are used almost exclusively for businesses and interoperate cooperatively with platforms. Personal analytics tools are geared toward analyzing the state of one's personal online life.

The most well-known commercial analytics tool is Sprinklr Social, a software-as-a-service company that helps businesses with their marketing and customer service needs. The product seeks to help businesses create, manage, and optimize their social media interactions with customers. Sprinklr offers features such as AI-driven analytics, social listening (i.e., real-time access to a large repository of publicly available data), and hashtag optimization.

While brands may be comfortable paying significant sums for detailed analytics—part of those fees accrue to the platform in API usage fees—individuals seeking an understanding of their social media performance generally expect to pay much less or nothing at all. Reports+, developed by GopGop Apps, is a

popular personal analytics tool compatible with Instagram, which has 339,000 ratings on the Apple Store and is currently 33rd on the social networking charts. The application offers various features, including some that most such tools have, like “secret admirers,” which allow a user to see who is viewing their profile, and “ghost followers,” which do not interact with content and are likely fake or bot accounts. This product also promises to inform the user when an account has been reactivated or disabled and includes a profile discover feature that allows one to locate any account with auto-complete suggestions.

However, warnings have appeared online about the dangers of this product: Some report that the app collects the user’s Instagram login credentials—a serious security risk—and it logs the user out of their Instagram session. Both claims, if true, suggest that Reports+ may be using methods to access Instagram data that would not be endorsed by Meta and may be blocked over time. It is easy to imagine ways in which a tool like Reports+ could be abused, with content creators pursuing their “secret admirers” and demanding they follow to increase the user’s follower count and presumably their revenues.

### *User experience tools*

To improve users’ experience on a given platform, user experience tools provide them with affordances to consume content in a manner distinct from the platform’s default—e.g., by changing the appearance of the type used by an application or altering its recommendation system. User experience tools are almost exclusively designed for those who seek control over the type of content they consume or the interface they engage with but do not post content to a server or modify it. They change the experience for a specific individual user and thus are designed for personal use. This increased control over user experience—particularly when it affects what content a user does and does not encounter—can meaningfully impact how a social media site affects a user, a user’s interactions with other users, and democratic discourse as a whole.

Tournesol, a great example of a user experience tool, aligns with the vision Fukuyama et al. (2021) put forth for middleware: a tool that algorithmically alters the content a user is exposed to. The product is an open-source, participatory research platform where users compare YouTube videos on Tournesol’s website to create a community-based recommendation algorithm. This algorithm is accessible while using YouTube with Tournesol’s browser extension.

Because Tournesol’s (n.d.) goal is to “advance research in the ethics of algorithms and recommendation systems,” the product does not directly earn revenue, although donations are accepted. Tournesol can be considered either a middleware “helper” app or an alternative client. As a helper app, it enables users to watch the community-recommended content on YouTube with a browser extension; as an alternative client, it enables users to watch and compare videos directly on Tournesol’s website. As a research project, Tournesol defaults toward making a user’s comparisons on their site public, unless configured otherwise.

While we have found no evidence of YouTube having taken action against Tournesol, we can imagine situations in which it might resent the power of the

new software. For example, since Tournesol's recommendations are less "sticky" than YouTube's, users might engage in briefer sessions and view fewer ads on the site. Tournesol reveals the power of middleware: A community-based algorithm can help solve the fact that "battles over social media are rooted in the sense that the people and processes governing online spaces are unaccountable to the communities that gather in them" (Zuckerman and Rajendra-Nicolucci 2023).

## Middleware and Platform Power

Our team has come to describe middleware as a feature request with teeth. Tracy Chou could have communicated her experiences with harassment to Twitter and might have been invited to participate in conversations about improving blocking, but there is no guarantee her input would have led to meaningful change.<sup>3</sup>

By creating middleware, Chou and her team upended an equation in which users have very little power. With Block Party, users now had access to a feature that Twitter either had not gotten around to implementing or had consciously chosen not to. At any point, platforms could put middleware providers out of business by incorporating middleware features into their core software. This is a time-honored strategy sometimes called "embrace and extend" (Markoff 1996), in which companies like Microsoft and Apple incorporate the function of popular software extensions into subsequent versions of their operating systems, undercutting the market for third-party tools.

Platforms can respond to middleware in at least three ways. First, they can embrace the additional functionality and celebrate the fact that new features are available that they did not need to develop or do not need to maintain. While this is an uncommon reaction, we see evidence that some of the analytic tools we document, such as Sprinklr Social, have been embraced, most likely because the providers of those tools pay significant sums to platforms for access to their API. Second, platforms can take an indifferent stance to middleware tools, neither embracing nor fighting them. Or, third, platforms can actively seek to undermine middleware tools either through legal or technical means.

When a platform seeks to undermine middleware through technical means, middleware tools often engage in "adversarial interoperability" (Doctorow 2023). In other words, the middleware author chooses to interoperate with the platform despite the platform's objections. As Cory Doctorow has documented in his writings about adversarial interoperability, this is a strategy with a long history in the tech industry: Apple-built word processing, presentation, and spreadsheet tools that were adversarially interoperable with Microsoft's software allowed Apple to hold onto a small slice of the business software market.

Profit is not the only reason companies can be adversarial to middleware tools. Concerns over third-party data access have also historically played a role. In one famous example, the political consultancy Cambridge Analytica scandal, a personality quiz, "Your Digital Life," developed by data scientist Aleksandr Kogan, used the Facebook Graph API to collect information on 87 million users of the

platform (Hern and Cadwalladr 2018). Kogan then gave the data to Cambridge Analytica, which used the data to target political ads in the U.S. and UK. Resulting outrage led Facebook to sharply constrain the data accessible to third-party developers.

Facebook's reasons for limiting data access are understandable, but their decision has created an environment in which platforms often assume ill intent from third-party developers and limit access to their systems to mitigate the danger that outside software can pose.

These two cases demonstrate that there is a spectrum of merits in adversarial interoperability. On one end, it can be a powerful tool for addressing power imbalances between developers, users, and platform owners. For instance, Chou and Block Party could have pursued an adversarially interoperable strategy when Twitter's API became unaffordable, writing software that interacted with the platform through scripts rather than making authorized API calls. Our lab is working on reproducing the functionality of Unfollow Everything, a middleware product designed by Louis Barclay, to automate the process of unfollowing users on Facebook. Because Facebook's API does not permit this form of mass unfollowing, our programming approaches are necessarily adversarial (Zuckerman 2024).

On the other end of the spectrum, there are cases in which it is easy to see arguments in favor of platforms that want to block middleware. Consider Grayjay, a product developed by FUTO. By aggregating video content from eight platforms into its own feed, Grayjay, rather than the apps or websites provided by the individual platforms, becomes the user's video interface. Changing the "point of service" has implications beyond user experience. For example, when viewing YouTube content through Grayjay, ads are blocked, which means YouTube no longer makes money. Furthermore, YouTube creators who share ad revenues with YouTube also no longer earn money when viewers use Grayjay.

Because Grayjay undermines YouTube's business model, YouTube's lawyers likened Grayjay to an outlaw (Mason 2024) and sent them two cease and desist letters. Their message is clear: Grayjay violates their API terms of service by using their content without permission. However, Grayjay has not relented, arguing that YouTube's claims are moot since Grayjay does not access YouTube's API. Grayjay has not elaborated on exactly how they access YouTube's content but most likely parses YouTube data by "screen scraping" (i.e., retrieving a webpage and analyzing the HTML to collect data).

YouTube lawyers argue that Grayjay should be proscribed because it is a one-time payment model that monetizes content without compensating content creators. And other platforms could argue they are similarly wronged by Grayjay. Nonetheless, Grayjay has positive features. An open-source tool, it gives users control over sorting content, allows them to store their watch history locally, and can operate with popular video-sharing apps.

With Grayjay in mind, we can see how it is possible to be pro-middleware and legitimately concerned about specific middleware products and their implications. When middleware overrides the business decisions made by platforms, advertisers, and creators, it's reasonable to ask whether platforms should be forced to interoperate. Still, even as we acknowledge these cases, we see many

more in which it makes good sense to make room for middleware and to foster a regulatory environment that recognizes its potential in parallel with other approaches to governance.

For middleware to become a better-established and more reliable tool, we need a policy environment that requires platforms to enable some types of interoperability. The precise boundaries of that interoperability require a stakeholder analysis—that is, a close look at what specific pieces of middleware mean to do and who is affected by the new capabilities middleware makes possible.

The following straightforward stakeholder analysis considers the initial version of Block Party, which existed between 2018 and 2022, before Twitter's API changes. The design enabled users of seven platforms to block harassers *en masse* if they chose to install the Block Party plug-in.

We consider costs and benefits for a set of possible stakeholders:

- Users of the software benefit by having a more civil and welcoming online experience.
- Advertisers likely benefit because their brand content is not associated with online harassment.
- Platforms benefit because blocking users helps them identify troublemakers and content likely to harm “brand safety.”
- Harassers are harmed in that their ability to engage in their preferred form of speech is blunted.
- Users as a whole may benefit as harassers find the affected platform a less receptive space for online harassment.

Our analysis of Block Party suggests a largely win-win scenario, in which everyone but harassers benefit from the application of middleware. However, not all scenarios are as clear-cut.

Take, for example, the case of Grayjay. There, users benefit because they can view videos without ads. But Grayjay is often harmful for video creators, who benefit from revenue-sharing arrangements with platforms. Platforms are harmed because they lose their primary way to generate revenue. Advertisers, too, are harmed because they can no longer reach targeted customers. Finally, Grayjay benefits from its one-time payment model.

The Grayjay stakeholder analysis requires us to decide whose stake matters most. For the founders of Grayjay, advertising is an inherently undesirable way to support online creativity. They reject the importance of advertisers and platform preferences and implicitly suggest that creators would benefit from moving to a different business model, i.e., subscription.

We argue that Grayjay's reasoning is faulty. The app will monetarily benefit only the small number of content creators on subscription-based platforms interoperable with Grayjay and not on YouTube. For Grayjay to benefit most creators, a future is required where most users and creators are on subscription-based platforms, not on YouTube. Relying on this future is not only a dangerous bet but also ignores all those creators who could be harmed now, not to mention those who advertise on YouTube.

So, at the very least, if a product (e.g., Grayjay) controls a content creator's content without their consent, policymakers should look at that product and its model skeptically. However, the boundaries get fuzzier when we look to the most critical actors in a stakeholder analysis: content creators or users. For example, if Grayjay had the same functionality with the qualification that videos on their site must have the consent of the content creator, should the product be able to exist? On the one hand, it takes away revenue from the originating platform and advertisers without their consent. But, taking away revenue from a platform through adversarial interoperability without the platform's permission is nothing new: Facebook did not ask Myspace to allow Facebook users to message Myspace users (Doctorow 2019).

We see this undercutting of a business model as well with the advent of ad-blocking plug-ins for web browsers, arguably the first widespread internet middleware. Such tools challenge the most common online business model: freely accessible content or services supported by targeted advertising. Despite significant objections by publishers like Axel Springer, German courts have widely found that ad blocking is permissible, a ruling that suggests that similar approaches to adding or removing functionality via middleware might be legally protected (Reuters 2018). However, legal uncertainty around middleware tools in general, and specifically around tools that affect revenue models, likely acts as a disincentive to invest in this space and points to the need for a more robust legal regime to enable middleware development.

## Building an Enabling Environment for Middleware

One study of middleware (Brickman 2025) suggests that middleware is not a theoretical solution to some problems of online governance but rather an actual and existing approach that we can evaluate and problematize. While middleware exists, creating it is still a fraught process for many developers due to uncertainty in the legal environment surrounding these tools. In embracing middleware as part of the internet governance solution, policymakers would need to advocate for an enabling environment, which would likely include the following:

- A requirement that platforms above a certain size maintain an API that is accessible and affordable to a wide range of developers. This might require platforms to demonstrate internal costs associated with particular operations and price API operations at a reasonable multiple of cost. For example, if it costs a platform \$0.0001 to delete a user's account, it could not charge an API user \$1 for making a similar API call.
- A mechanism through which users could access all content they are "entitled" to access on a platform (i.e., content from users they are friends with or subscribed to), independent of filtering provided by a platform's algorithms.

- A recognition of protected uses of middleware, which would include, at minimum, privacy enhancement, accessibility for users who are blind or deaf, and user control over content recommendation and filtering algorithms. The social benefits of these protected uses would be taken into account when considering the tensions between possible revenue losses to platforms and increased benefits for users.

The goal of such a regime would be to reduce legal and commercial risk for middleware developers, allowing increased investment in the field. At present, it is difficult for middleware companies to secure investment due to the risk that new products may be blocked technically or litigated into nonexistence. Creating a climate of reduced risk for middleware could bring about diverse offerings, such as Fukuyama's fact-checking proposal.

We argue that an environment should be regulated by Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), which prohibits "unfair or deceptive acts or practices in or affecting commerce." *Unfair* and *deceptive* are independent of each other. In this context, unfair means substantial injury that is unavoidable and not outweighed by benefits to consumers or competition, and deceptive means a material, misleading representation that is reasonably interpreted by the consumer.

There are four potential outcomes of an FTC investigation into a middleware product:

- (1) the agency's decision to close the investigation,
- (2) a settlement between the FTC and the target of the investigation,
- (3) the agency's filing of an administrative complaint, or
- (4) the agency's filing of a complaint in federal district court. (Reicher and Fang 2016, 2–3)

Grayjay offers a thought experiment in how FTC regulation might work in practice. Grayjay is unlikely to be accused of deceptive practice, but Google/YouTube is already arguing that it is engaged in unfair practices. The FTC could find that the benefits Grayjay brings to consumers—the ability to sort content, the aggregation of platforms, challenging YouTube's primacy in the video marketplace—outweigh Grayjay's harms. In that case, the agency would close the investigation. Conversely, the FTC could find that the harms—undercutting the creator economy, taking away advertiser revenue—outweigh the benefits. In this scenario, a settlement, an administrative complaint, or a filing in federal district court is possible. These three actions would keep the door open for legal remedies, which could include forcing Grayjay to shut down, changing their affordances, and/or paying YouTube for monetary damages.

We believe that the right to control our experience of the internet is already granted as part of the Communications Decency Act of 1996 (47 U.S.C. § 230(b)), which states in part:

It is the policy of the United States—

- (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

- (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
- (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
- (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.

Our argument that a federal court should enjoin Meta from blocking a new version of Unfollow Everything relies on an interpretation of 230(b) as recognizing the importance of middleware, particularly the form that allows users to filter content as they choose. A federal court has invited us to resume our case once we have produced working code that implements the Unfollow functionality. Meta has taken many steps that make producing such software quite difficult. While a finding in our favor would not prevent Meta from making it difficult for us to accomplish our goals (by failing to provide API functionality, obscuring code, etc.), it would recognize the legitimacy of our strategy of using middleware software to control user experience of online content.

## Conclusion

We believe that a legal regime that recognizes middleware and its importance begins with an understanding that middleware is a real and existing approach to online governance, not a theoretical future. By documenting middleware as it exists, we seek to open a broader conversation about online governance approaches.

Our support of middleware is part of a larger vision, where we advocate for a plurality of different social media platforms that either interoperate directly or can be read from and written to using aggregators like Gobo.social. These aggregators would enable the use of middleware tools that users could use to enhance privacy and filter content in whatever ways are most beneficial for them.

We see middleware as an imperfect avenue for reform, complementary to other imperfect moderation strategies. If middleware is to be widely utilized, its applications should do more good than harm. Therefore, we advocate for the use of stakeholder analysis (which considers the positions of all major actors involved) to help gauge what middleware products and features are helpful and harmful and suggest a framework for regulation. Such a framework is needed, as laws or litigation informed by such a framework seem like prerequisites to creating healthier social media ecosystems. The examples above show that some existing middleware programs can be harmful, and that helpful ones (which often require API access), are not always allowed by the platforms.

Our ambitions for middleware are not modest. We advocate for, and are building, a social media system with numerous competing platforms, highly customizable aggregators that users control, and a robust marketplace for middleware that users can choose to adopt to shape their social media experience. In our vision, users could choose more or less moderated versions of the same platform, based on shared whitelists and blocklists like Block Party. Using apps like Tournesol, users would select algorithms to meet their needs for filtering and prioritizing content they encounter. While we do not pretend that middleware can solve all problems associated with platform governance, we believe it is a powerful and underutilized tool that avoids many of the issues of platform compliance or government intrusion into speech. Critically, we see a need for the visibility of middleware as a complement or an alternative to other governance interventions so that more users know what tools already exist, more developers take up the task of solving problems with middleware, and platforms and regulators accept middleware as an established part of the social media landscape.


## Notes


1. In some instances, the lower courts might find that the government has the right to regulate platforms based on First Amendment interests, particularly in the case of platforms that provide business services, a sector where a presumption of nondiscrimination prevails.

2. This quote is sometimes attributed to Andrew Lewis (2010), who, in turn, sees the origins of the quote as with the artist Richard Serra, decades earlier (O'Toole 2017).

3. The experience of one of the authors of this article (Zuckerman) is instructive: Once a heavy Twitter user, he flagged his experiences as an alcoholic in recovery who was encountering unblockable ads for liquor on the platform. The site's revenue team responded, promising to look into creating a feature that would allow users to block alcohol advertising (Zuckerman 2021), but nothing of the kind was ever implemented.

## ORCID iDs

Ethan Zuckerman  <https://orcid.org/0000-0002-5970-9116>

Isaac Brickman  <https://orcid.org/0009-0007-0955-0577>

## References

- Associated Press. 7 August 2024. Zuckerberg says the White House pressured Facebook to “censor” some COVID-19 content during the pandemic. *PBS News*. Available from [www.pbs.org](http://www.pbs.org).
- Bhargava, Rahul, Anna Chung, Neil S. Gaikwad, Alexis Hope, Dennis Jen, Jasmin Rubinovitz, Belén Saldías-Fuentes, and Ethan Zuckerman. 2019. Gobo: A system for exploring user control of invisible algorithms in social media. In *CSCW '19 companion: Proceedings of the 22nd ACM conference on computer supported cooperative work and social computing*. Association for Computing Machinery.
- Bond, Shannon. 23 February 2021. Block Party aims to be a “spam folder” for social media harassment. *NPR*. Available from [www.npr.org](http://www.npr.org).
- boyd, danah. 31 January 2024. KOSA isn't designed to help kids. *Zephoria* (blog). Available from [zephoria.medium.com](http://zephoria.medium.com).

- Brickman, Isaac. 2025. *A taxonomy of middleware: How user tools can improve social media*. Initiative for Digital Public Infrastructure, University of Massachusetts Amherst. Available from publicinfrastructure.org.
- Chou, Tracy. 11 October 2013. Where are the numbers? *Triketora* (blog). Available from medium.com/@triketora.
- Communications Decency Act. 1996. 47 U.S.C. § 230 – Protection for private blocking and screening of offensive material.
- DiResta, Renee. 2018. Computational propaganda: If you make it trend, you make it true. *Yale Review* 106 (4): 12–29.
- Doctorow, Cory. 7 June 2019. *Adversarial interoperability: Reviving an elegant weapon from a more civilized age to slay today's monopolies*. *Deepinks* (blog). Electronic Frontier Foundation. Available from www.eff.org.
- Doctorow, Cory. 2023. *The internet con: How to seize the means of computation*. Verso.
- Federal Trade Commission Act. 1914. 15 U.S.C. § 45 – Unfair methods of competition unlawful; prevention by Commission.
- Freelon, Deen, Charlton D. McIlwain, and Meredith D. Clark. 2016. *Beyond the hashtags: #Ferguson, #Blacklivesmatter, and the online struggle for offline justice*. Center for Media & Social Impact, School of Communication, American University. Available from cmsimpact.org.
- Fukuyama, Francis, Barak Richman, Ashish Goel, Roberta R. Katz, A. Douglas Melamed, and Marietje Schaake. 2021. *Middleware for dominant digital platforms: A technological solution to a threat to democracy*. Cyber Policy Center, Freeman Spogli Institute, Stanford University. Available from https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/cpc-middleware\_ff\_v2.pdf.
- Gill, Nicole. 1 July 2024. Accountable Tech statement on Supreme Court content moderation cases. *Accountable Tech*. Available from accountabletech.org.
- Hendrickx, Jonathan, and Michaël Opgenhaffen. 2024. Introduction: Understanding social media journalism. *Journalism Studies* 25 (9): 919–930.
- Hern, Alex, and Carole Cadwalladr. 13 April 2018. Revealed: Aleksandr Kogan collected Facebook users' direct messages. *Guardian* (U.S.).
- Hirschman, Albert O. 1970. *Exit, voice, and loyalty: Responses to decline in firms, organizations, and states*. Harvard University Press.
- J, Vaishnavi. 20 March 2024. Why is KOSA so popular and what does it mean for child safety regulation in the US? *Tech Policy Press*. Available from www.techpolicy.press.
- Kids Online Safety Act. 2023. S.1409, 118th Cong.
- Lane, Spencer. 9 November 2022. Gobo 2.0: All your social media in one place. *Initiative for Digital Public Infrastructure* (blog). Available from publicinfrastructure.org.
- Lewis, Andrew (@andlewis). 13 September 2010. "If you are not paying for it, you're not the customer; you're the product being sold." X. https://x.com/andlewis/status/24380177712.
- Mac, Ryan, and Cecilia Kang. 3 October 2021. Whistle-blower says Facebook "chooses profits over safety." *New York Times*.
- Markoff, John. 16 July 1996. Tomorrow, the world wide web! Microsoft, the PC king, wants to reign over the internet. *New York Times*.
- Mason, Ian. 17 April 2024. Grayjay response. Response on behalf of FUTO to a January 25, 2024, email sent to Peter Mahaffey. Letter on file with FUTO, Austin, TX. Available from https://futo.org/legal/Grayjay-Response.pdf.
- Moody v. NetChoice, LLC. 2024. 603 U.S. 707.
- Morris, Betsy. 2024. *Battle for privacy: The case of Block Party*. McCoy Family Center for Ethics in Society, Stanford University. Available from ethicsinsociety.stanford.edu.
- Mosleh, Mohsen, Qi Yang, Tauhid Zaman, Gordon Pennycook, and David G. Rand. 2024. Differences in misinformation sharing can lead to politically asymmetric sanctions. *Nature* 634 (8034): 609–616.
- O'Toole, Garson. 16 July 2017. Quote origin: You're not the customer; you're the product. *Quote Investigator*. Available from quoteinvestigator.com.
- Pariser, Eli. 2011. *The filter bubble: What the internet is hiding from you*. Penguin Press.
- Perez, Sarah. 11 March 2024. After losing access to Twitter's API, Block Party pivots to privacy. *TechCrunch*. Available from techcrunch.com.

- Rajendra-Nicolucci, Chand, Michael Sugarman, and Ethan Zuckerman. 2023. *The three-legged stool: A manifesto for a smaller, denser internet*. Initiative for Digital Public Infrastructure, University of Massachusetts Amherst. Available from [publicinfrastructure.org](https://publicinfrastructure.org).
- Reicher, Alexander E., and Yan Fang. 2016. FTC privacy and data security enforcement and guidance under section 5. *Competition* 25 (2): 115657.
- Reuters. 19 April 2018. German Supreme Court rules ad blockers legal, in defeat for Springer.
- Scott, Mark, and Oliver Marsh. 20 February 2025. The Musk effect: Assessing X's impact on Germany's election discourse. *Digital Forensic Research Lab* (blog). Available from [dfriab.org](https://dfriab.org).
- Social media platforms. 2021 (enacted). SB 7072, Florida Senate.
- Starbird, Kate, Renée DiResta, and Matt DeButts. 2023. Influence and improvisation: Participatory disinformation during the 2020 US election. *Social Media + Society* 9 (2): 20563051231177943.
- Sunstein, Cass R. 2017. *#Republic: Divided democracy in the age of social media*. Princeton University Press.
- Tournesol. n.d. Frequently asked questions. Available from <https://tournesol.app/faq>.
- Tufekci, Zeynep. 2017. *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.
- Wardle, Claire, and Hossein Derakhshan. 2017. *Information disorder: Toward an interdisciplinary framework for research and policy making*. Report DGI(2017)09. Council of Europe. Available from <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>.
- Zuboff, Shoshana. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.
- Zuckerman, Ethan. 2014. New media, new civics? *Policy & Internet* 6 (2): 151–168.
- Zuckerman, Ethan. 18 February 2021. Hey Twitter, I need it not to be Bourbon Time. *Ethan Zuckerman* (blog). Available from [ethanzuckerman.com](https://ethanzuckerman.com).
- Zuckerman, Ethan. 5 May 2024. I love Facebook. That's why I'm suing Meta. *New York Times*.
- Zuckerman, Ethan, host. 15 May 2025. Deleting everything with Dan Saltman. Episode 113. *Reimagining the Internet* (podcast). 46 min., 6 sec. Available from <https://publicinfrastructure.org/podcast/113-dan-saltman>.
- Zuckerman, Ethan, and Chand Rajendra-Nicolucci. 24 October 2023. Let the community work it out: Throwback to early internet days could fix social media's crisis of legitimacy. *Conversation*. Available from [theconversation.com](https://theconversation.com).