Center on Regulation and Markets at BROOKINGS

POLICY BRIEF | MAY 2023

TIKTOK SHOWS WHY SOCIAL MEDIA COMPANIES NEED MORE REGULATION

THEY POSE A THREAT TO NATIONAL SECURITY, AMERICANS' PRIVACY, AND CHILDREN'S HEALTH

SANJAY PATNAIK AND ROBERT E. LITAN

Executive Summary

There has been increasing political awareness regarding the national security issues posed by TikTok, the popular social media app owned by Chinese company ByteDance. Lawmakers and the public are right to be concerned—numerous data points are now available, from ByteDance's connections to the Chinese Communist Party to its potential for social manipulation to its gathering of American personal data. Some efforts have been made to limit the potential risks, for example storing TikTok data on U.S. (rather than Chinese) servers. However, more could be done. Additional measures should also be considered by lawmakers, including the forced sale of ByteDance's U.S. operations or even a complete nationwide ban on TikTok.

TikTok's national security threat is only one component of the myriad challenges facing regulators looking to protect citizens utilizing social media platforms. For that reason, TikTok is a useful case study to examine broader issues with social media at large. TikTok and other social media platforms, including Instagram and Facebook, often have adverse effects on the mental health of minors. Unrealistic beauty standards, bullying, and sexual harassment are all very real problems on these platforms, and policymakers should do more to encourage the companies to seek solutions. Additionally, mis- and dis-information often run rampant due to social media companies' varying and often lax rules on content moderation, which can pose a particular challenge to American democracy when a social media company is under the influence of a foreign adversary.

Holding social media companies accountable is difficult under present law, most notably due to Section 230 of the Communications Decency Act, which provides broad legal liability protections to companies for content their users post. Additionally, ensuring that U.S. user data is secure and cannot be exploited by foreign adversaries may require CFIUS to make a recommendation either leading to the forced sale of TikTok or banning the platform altogether. We explore policy solutions to the aforementioned issues, including passing an updated data protection law, incentivizing the development of better age verification practices by social media companies, and re-establishing a "duty of care" standard requiring companies to take reasonable steps to prevent harm to users.

Introduction

In less than two decades, social media has become a near-ubiquitous presence in modern life, currently used by over 70% of U.S. adults. It is especially popular among teens, who reportedly spend an average of five to seven and a half hours per day on social media. As many as 38% of children aged 8-12 are using social media despite formal age restrictions on most major platforms. TikTok is the fastest-growing social media company in the U.S. with over 100 million active U.S. users each month, a number that is up 800% since January 2018. In 2021, its users spent an average of 99 minutes on the app per day. TikTok was also the most popular social media platform for U.S. teens in 2022.

Despite the potential benefits of social media connecting people and facilitating the dissemination of useful information, concerns about the negative effects of social media use in general, especially on our youth, have risen significantly in recent years. In this context, TikTok provides a particularly salient example for why the lack of regulations and oversight of social companies in the U.S. can be highly problematic. While the major threat TikTok poses is to U.S. national security due to its Chinese ownership and reported ties to the Chinese government, these issues only aggravate more general problems that social media platforms owned by U.S. companies also present for American citizens and policymakers. These problems include social media's detrimental effects on the mental well-being of many users, especially younger ones; its ability to help spread misinformation; and its large contribution to the erosion of personal privacy. TikTok can serve as an important case study for why the U.S. needs to tighten its regulations of social media companies with regard to (1) specific risks of foreign ownership by adversaries and (2) broader detrimental effects of social media that are amplified if a social media company is under the influence of an autocratic regime.

TikTok is widely seen as a serious national security threat for several reasons. For one, ByteDance, TikTok's parent company, collects extensive data from its users, and the app stores detailed information about users' preferences. TikTok's data collection activities have triggered major concerns at a time when the U.S. is increasingly wary of China's rise as a geopolitical adversary and the Chinese government has been tightening its grip on its tech industry. ByteDance has reportedly considered using TikTok to monitor the locations of specific U.S. citizens, and the FBI has said that China itself could use TikTok to spy on Americans and U.S. government workers.

An additional threat arises from TikTok's potential as an information (or misinformation) disseminator. There have been numerous allegations that TikTok is under the influence of the Chinese government, which would exacerbate the danger it can pose by spreading misinformation and by facilitating the potential for the Chinese government to promote propaganda. Misinformation and polarizing content are routinely promoted by social media at a higher rate than other content providers like search engines such as Google. Indeed, misinformation has been rampant on various social media platforms, including TikTok and Facebook. Russia's misinformation campaign to influence voters before the 2016 election exemplifies the risks of misinformation on social media, which would be significantly heightened if the platform itself was owned or influenced directly by an autocratic, adversarial regime. Misinformation is especially problematic when it can affect the education and opinions of the social media platform's young user base, since a substantial portion of young Americans now receive news on TikTok. Young people may be a likely target of influence campaigns by the Chinese government.

TikTok and other social media companies have also come under scrutiny for their adverse impact on children. Other social media platforms like Facebook, Instagram, and Twitter are generally better-researched with respect to their impacts on teens' self-esteem, online bullying, dangerous trends that influence behavior, potential for social media addiction, and children's privacy. Research about TikTok's impacts in these areas is in its early stages. Several state attorneys general are investigating what TikTok knows about the app's negative effect on young people's mental and physical health and whether the company has knowingly utilized tools to boost engagement with the app despite these health impacts. Research has shown that underregulat-

ed social media at large can promote anorexia and that the TikTok algorithm in particular often recommends self-harm and eating disorder content to some teens within minutes of an account's activation.

Not surprisingly, Congress is currently considering a number of legislative responses, including the bipartisan RESTRICT Act, which would give the Department of Commerce authority to ban or limit technology developed by Chinese firms that may pose a security threat, including TikTok. As with automobiles, which have positive benefits but also pose serious dangers and therefore are regulated, social media also merits cost-effective regulation that preserves the benefits and limits the risks. Toward that end, in this report, we discuss first the current problems with social media in general and the reasons why it merits more stringent regulation. We then outline the existing domestic and international regulatory frameworks that purport to control the negative side effects of social media platforms. We conclude by recommending certain ways in which the dangers of TikTok can be addressed in the short run, as well as how new legislation would better minimize the downsides of social media in the long run.

TikTok's National Security Risks

There are multiple reasons for regulating ownership of social media companies by international firms based in adversarial nations with autocratic regimes that the TikTok example highlights, including political interference resulting from misinformation that can be steered by an authoritarian regime.

The vast quantities of data that TikTok collects may allow it to become an instrument of political interference in the U.S. through disinformation or propaganda campaigns that target U.S. voters. This could happen either through direct Chinese government influence on TikTok and the algorithm that promotes, hides, and even censors certain content over others or by the Chinese government creating content for other social media sites that utilizes TikTok user data to target political ads to American citizens, similar to Russia's election interference campaign in 2016. (We now know that of the hundreds of thousands of social media accounts Russia's government has created, the Russian operators of those accounts have boasted that only 1% of them have been detected.)

Concerns over foreign influence in elections drove, in part, an early bipartisan request by Senators Chuck Schumer (D-NY) and Tom Cotton (R-AR) for a national security investigation of TikTok. Republican lawmakers have recently argued that TikTok could use its algorithm and user data to "subtly indoctrinate" American citizens, citing TikTok's reported censorship of politically sensitive content critical of the Chinese government.

Indeed, ByteDance's founder and former CEO validated these concerns when he publicly promised to support Chinese Communist Party ideology in a 2018 statement. Leaked content moderation documents obtained by the British newspaper the Guardian demonstrated TikTok's censorship of videos in line with Chinese foreign policy, such as videos about Hong Kong protests or Tibetan independence. Former ByteDance employees also claimed that an English-language ByteDance news app pushed pro-China content, a claim that was denied by the company. Further, a Forbes investigation found that large numbers of current and former ByteDance and TikTok employees had worked for Chinese state media.

In further support of these concerns, a recent report submitted by a group of researchers to the Australian Senate Select Committee on Foreign Interference through Social Media concluded that ByteDance's promotion of government propaganda through its Chinese app generated "material risk that they could do the same on TikTok." The report also found that TikTok has been an active participant in China's military-industrial-surveillance complex, and that ByteDance is deeply enmeshed with the Chinese Communist Party.

In sum, between ambiguous Chinese laws that could allow the Chinese government to lay claim to data stored within the country and ByteDance's own actions indicating a lack of robust, transparent measures to protect user information, China could utilize TikTok data in ways that could pose a national security threat to the United States.

Like many other social media companies, the TikTok platform has been a source of political mis- or disinformation. While there are no easy regulatory solutions for misinformation spread on social media that do not run afoul of the First Amendment, the TikTok case is different because it concerns speech that is being filtered through a foreign adversary (as the company is under the influence of the Chinese regime which could use TikTok to spread misinformation beneficial to goals of the Chinese government). The best way to address that legitimate concern would be to limit the ownership and influence from autocratic foreign governments over social media companies operating in the U.S.

The misinformation dangers presented by TikTok were illustrated during the recent Brazilian presidential election when TikTok searches pushed people towards false claims of election fraud. Similarly, before the 2022 U.S. midterm elections, TikTok failed to detect 90% of advertisements containing political disinformation that were submitted by a research group. Further, recent Reuters searches of political keywords on TikTok found search suggestions relating to false claims about mail-in voting and election candidates as well as conspiracy theories.

TikTok has also proliferated misinformation on a number of other political subjects. Infamously, TikTok facilitated the spread of misinformation regarding COVID-19, from vaccines to treatments, and on a wide range of other topics, such as climate change. These issues have occured despite TikTok's policies not allowing medical misinformation and misinformation about voting. In fact, reports have found that TikTok performs worse than other social media companies in terms of catching misinformation in advertisements. One study found that the social media site approved 90% of the ads the researchers submitted containing misinformation on voting. Facebook, on the other hand, caught 65% of the researchers' false advertisements, while YouTube caught 100% of the ads and suspended the account the researchers had set up for the study.

Most recently, the New York Times found that misinformation went relatively unchecked on TikTok leading up to the 2022 midterm elections, with hashtags like "#stopthesteallll" and videos containing debunked rumors about the January 6 attack on the Capitol Building being viewed extensively on the app. And although the app has taken down hundreds of thousands of videos with deepfake or false content, this appears to only be a small dent, with one study estimating that one in five TikTok videos contain misinformation. Teens are particularly susceptible to receiving this content and not checking it with other sources, since Gen Z is increasingly using TikTok as a search engine for news in place of other, more reliable sites.

Data Privacy and Security

In addition to the specific national security challenges of foreign-controlled political interference and misinformation on TikTok—and future foreign-owned social media companies—the lack of a robust federal privacy protection framework in the U.S. opens yet another vector of national security risks.

Social media platforms have repeatedly been found to be misusing user data. Facebook was fined $5 billion by the Federal Trade Commission (FTC) for selling users' "friend" data to third-parties in 2019. In 2022, the FTC fined Twitter $150 million for illegally profiting from "deceptively collected data."

With foreign-owned social media platforms, especially Chinese-owned TikTok, the misuse of user data takes on national security implications. TikTok collects a wide range of data on its users, such as identifying information like name, age, phone number, email address, IP addresses, and locations. TikTok's in-app browser reportedly collects user keystrokes. Indirectly, TikTok employs users' behavior and interactions to infer their interests, although this inference data is not made available to users themselves. By comparison, Facebook reveals to users what it has inferred about them, a long list of 98 data points that typically include political leaning, employer information, income level, and race/ethnicity. TikTok also may have biometric information of its users such as facial recognition and voiceprints drawn from user-uploaded video. Other experts have expressed concern that the Chinese government could execute campaigns to carry out intellectual property theft through its use of TikTok data. Theoretically, the

Chinese government could target TikTok users with access to sensitive intellectual property data and "phish" for information to gain access to this information through the app, targeting, for example, defense contractors or telecommunications employees.

Given the mountains of Americans' personal data collected by ByteDance, the Chinese owner of TikTok, Americans are right to be concerned about the consequences of this data falling into the hands of the Chinese government.

Apart from the growing strength of the China's authoritarian regime, the government's activities in tech pose specific concerns. In 2021, the government passed a law requiring the country's domestic technology companies to route all decisions regarding the security of "core state data" through the government's national security officials. Officials may demand access to such data from tech firms, and failure to comply can result in large fines or the revocation of a tech firm's operating license. "Core state data" is only loosely defined in the law as data that poses a "serious threat" to Chinese national security and categories of specific data that fall under this umbrella may continuously change. Experts say the law leaves room for the government to force domestic tech companies to report large amounts of user data to the government. Additionally, while this law contains some "data protection" provisions, importantly, the law does not limit the Chinese government's access to user data in any way.

Experts say that through its multiple tech-related actions, China is seeking to "expand extraterritorial control over digital platforms" and to "conquer" more digital territory through controlling user data. Large Chinese initiatives for global digital control include the Digital Silk Road Project that covers international technology cooperation and export, an expanding Chinese telecom and media footprint, and China's large and growing presence in global digital value chains. TikTok is the most prominent example of how China could potentially control U.S. user data. U.S. military branches and security agencies have banned the use of TikTok on official devices, and security concerns have been raised by senior officials such as the director of the Federal Bureau of Investigation as well as the deputy attorney general of the U.S. India banned TikTok in 2020, citing data security concerns amidst a 2020 border conflict with China. Ireland's Data Protection Commission launched an investigation into TikTok's data protection practices in 2021.

FBI Director Christopher Wray has warned that if TikTok user data falls into Chinese government's hands, China could weaponize the data for its political purposes. Weaponization can take various forms, from tracking of government employees to spying on the activities of individuals and corporations. Republican lawmakers Marco Rubio (R-FL) and Mike Gallagher (R-WI-8) have echoed these concerns.

Leaked records from TikTok in 2022 bolster these claims. The records showed that employees in China had accessed U.S. personal user data. Such claims had been made previously by former TikTok employees as well. Further, a recent update to TikTok's European privacy policy confirmed that employees in China have remote access to user data. A Forbes investigation revealed that Beijing-based TikTok employees were planning to track specific American citizens' locations through TikTok.

TikTok responded to earlier data privacy concerns by stating that a U.S.-based security team determined all data access and that the company would decline any request from the Chinse government for U.S. user data. Further, TikTok has stated that its U.S. user data was previously channeled only through the company's U.S. and Singapore data centers and is now being deleted from its own servers as it transitions entirely to using Oracle servers. However, TikTok recently declined to explicitly commit to ending all Chinese employee access to U.S. data. Among the most recent disturbing disclosures is that TikTok may have unlawfully surveilled U.S. journalists. The Department of Justice has opened an investigation into the matter.

In sum, while the unique national security challenges presented by foreign-owned social media like TikTok go beyond data privacy concerns, TikTok's case underscores the data privacy concerns presented by social media platforms more generally.

Youth Impacts

Beyond the national security and data privacy concerns raised by TikTok in particular, the often-addictive nature of the services provided by social media platforms more generally can pose threats to the mental and physical health of young people. TikTok's dangers, because the app is so widely used by young people, are especially concerning.

Pew research found that 63% of American children between 12 and 17 used TikTok in 2021. Further, one-third of TikTok's U.S. users are reported to be under 14. The UK's media regulator found that 16% of toddlers, or 3 to 4-year-old children, used TikTok, as did one-third of 5 to 7-year-old children. A report by NewsGuard found that children are also especially exposed to misinformation on TikTok.

Social media platforms are also often sites of sexual harassment of minors, as well as places where child sexual abuse content is shared. TikTok in particular, given its harder-to-moderate video format, rapid growth, and popularity among youth, has seen numerous reported cases of predators using it to meet children.

TikTok is the subject of numerous consumer protection investigations, past and present. The FTC fined TikTok for violating the federal Children's Online Privacy Protection Act (COPPA) with a $5.7 million settlement in 2019, in which the agency alleged that TikTok had illegally collected personal information from children. Specifically, the app was cited for recording the email addresses, names, and schools of users under the age of 13 and did not delete personal data even when implored by parents. This was found to be in direct violation of COPPA, which states that data collection from users under 13 requires permission expressly granted by their parents.

In its settlement agreement, TikTok agreed to implement certain child protection conditions, including the deletion of videos and data from users known to be under 13. Since the settlement, advocacy groups say that TikTok has violated these terms, refusing to delete content and data from these users. TikTok also entered a separate $91 million settlement agreement in early 2021 over additional claims of children's privacy rights violations and is the subject of a separate, ongoing Department of Justice investigation over its handling of child sexual abuse content.

As of this writing, a bipartisan group of state attorneys general is investigating whether TikTok has violated consumer protection laws regarding children's health. The group's investigation has been prompted by a larger trend of social media companies knowingly marketing to teens despite research showing the negative impact of many forms of social media engagement on teens' mental health, often resulting in lower self-esteem and increased rates of depression and anxiety among this age group. Most notably, at Instagram, a whistleblower who worked at parent company Meta leaked documents showing that the company was aware that Instagram exacerbates body image issues for one in three girls, and that 14% of boys reported feeling worse about themselves because of the social media platform. The research specifically found that Instagram's features, including its algorithm that selects content to display on its "explore" page, create a "perfect storm" to lower one's self-image. Even with this data, social media companies rarely take action to protect teens. In this case, despite this information appearing in a report to CEO Mark Zuckerberg, Meta did little to improve the situation.

Other experts have discussed the adverse effects of social media at large. Jonathan Haidt, who has written extensively about the effect of social media on teens' well-being, has connected heightened levels of self-consciousness seen in girls in the last ten years to the rise of social media. He has also demonstrated how social media has increased major depressive episodes among American teens, which in turn have increased suicide and self-harm rates. Still other studies have pointed to social media's emulation of gambling methods to "create psychological dependencies," physically altering the brain by playing on what grabs users' attention most and presenting them with unpredictable rewards to get them to habitually check their screens. This type of brain activity has been linked to increases in depression and anxiety.

Studies have shown similarly negative effects of TikTok on the well-being of young people. One study found that, among children with eating disorders, 59% reported that the app lowered their self-esteem, and another found that the algorithm can begin promoting content about depression, anxiety, and eating disorders within seconds of activating an account. Some doctors and experts have said that the app's content can worsen teens' mental health, although other experts say we know too little about TikTok's effect on the brain. These concerns most recently prompted the Indiana attorney general to file a lawsuit against TikTok, claiming that app is not safe for 13- to 17-year-olds. Further, in a 2020 report, leaked documents revealed that TikTok's content moderators were instructed to suppress "posts created by users deemed too ugly, poor, or disabled for the platform." Such suppression may contribute to mental health issues by fostering unrealistic beauty standards, in addition to being discriminatory.

The opacity of TikTok's data use and algorithms makes it difficult to assess the full scope of the platform's dangers. In concessions to concerns about content moderation and recommendation engines, in July 2022 TikTok announced it would provide some researchers with backend data access, including the independent experts on its U.S. Content Advisory Council. However, more such steps are needed, and regulators would benefit greatly from having greater access to TikTok's processes and algorithms.

Concerns about TikTok have also alarmed regulators abroad. In 2020, the Dutch Data Protection Authority submitted a report investigating digital grooming and online bullying on TikTok. It later fined TikTok €750,000 for not providing a privacy statement in Dutch, which it stated violated the privacy rights of young children. The European Commission has also engaged in extensive dialogue with TikTok about changing its practices after complaints emerged to the European Consumer Organization that the platform "failed to protect children from hidden advertising and inappropriate content." The Commission is seeking greater transparency into TikTok's business operations to better understand its impact on young users. In our policy recommendations section below we outline how U.S. regulators should be empowered to take similar measures in this country.

Current Policies Governing Social Media

Given the many challenges that social media presents for national security and consumer protection, regulators and lawmakers in many jurisdictions have begun developing a policy framework to curb the harms of social media. We concentrate here, however, primarily on the U.S. and the European Union.

UNITED STATES: EXISTING NATIONAL SECURITY POLICY TOOLS

The primary tool U.S. policymakers have used to attempt to address the national security challenges associated with foreign investment in social media companies is the Committee on Foreign Investment in the United States (CFIUS). We have discussed the structure, history, jurisdiction, and case law of CFIUS in a previous article. Here, we briefly cover the applicability of CFIUS powers to TikTok, and specifically how the committee could play a role in preventing future foreign influence in any social media company through mergers and acquisitions.

CFIUS's broad role is to "review certain transactions involving foreign investment in the United States and certain real estate transactions by foreign persons, in order to determine the effect of such transactions on the national security of the United States." CFIUS's jurisdiction covers foreign investments in U.S. companies. TikTok's history reveals the grounds for CFIUS intervention.

The Chinese company ByteDance launched a short-video app in 2016, primarily for the Chinese domestic market, and subsequently released an international version of this app called TikTok. In 2017, ByteDance acquired Musical.ly, a Chinese company with a strong U.S. presence including an office in California, and merged it into TikTok in 2018. This acquisition is considered a "foreign investment," thereby enabling CFIUS to review the case.

TikTok is also subject to CFIUS review by recent legislation and regulation. Under the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018 and its associated regulations, "sensitive personal data" of U.S. persons is considered a strategic asset, and investments that may give foreign parties access to such data is subject to a national security review. Thus, the reported Chinese access of U.S. data provides the primary grounds for CFIUS to scrutinize TikTok, and potentially order the divestiture of its U.S. business.

President Biden has specifically directed CFIUS, by executive order, to consider cybersecurity risks to election security, a potential additional basis for the investigation of TikTok. CFIUS did in fact open an investigation into TikTok in 2019, following bipartisan requests. While CFIUS review prompted President Trump to attempt to ban the app, TikTok successfully convinced a court to block this ban, which ruled that the government had not considered other alternatives. Potential deals to sell all or part of TikTok to a Microsoft-Walmart coalition and Oracle subsequently fell through.

In an effort to reduce further CFIUS scrutiny, TikTok says that all U.S. user data is now routed through independent Oracle servers,[1] and a dedicated Oracle team will be involved in data handling oversight. A security deal as part of a negotiated settlement with CFIUS reportedly may involve an independent board and auditors for the U.S. operations of TikTok. Most recently, the Biden administration has reportedly demanded that ByteDance divest TikTok or be faced with a ban, as a part of CFIUS proceedings.

The case of TikTok therefore reveals that CFIUS investigation can lead to forced divestitures and the implementation of mitigation measures and security deals related to data sovereignty. CFIUS reviews are thus likely to be a useful tool in addressing national security threats of foreign-owned social media platforms.

1 TikTok currently uses its own servers in the U.S. and Singapore as backups, and though the company says it plans to phase out its own servers so that all U.S. data is solely stored in independent servers, it has not done this yet. Cybersecurity experts continue to warn that TikTok's data is not reliably secure.

In addition to CFIUS action, an amendment to Section 310 of the Communications Act of 1934 could also authorize actions to curtail foreign influence in social media. To prevent excess foreign influence in traditional U.S. media (television and radio), this act prohibits any foreign government from holding a television or radio license and forbids foreign entities (individuals, companies, and governments) from holding more than a 20% stake in a broadcast carrier licensee or a 25% stake in a company that "directly or indirectly controls" such a licensee. The Federal Communications Commission can grant exceptions on a case-by-case basis after review, which it has done several times in recent years. It is important to note that this proposal would broaden the FCC's authority to social media platforms and change the nature of the FCC in a significant way, potentially raising obstacles to its implementation.

An alternative approach to regulating foreign social media platforms and technologies is being advanced in a recent set of bills in Congress that is designed to get around the Cold War-era International Emergency Economic Powers Act (IEEPA) of 1977. IEEPA empowers the president to restrict trade with hostile nations, but the Berman Amendments of 1988 exempt foreign information flows from presidential oversight. The bipartisan RESTRICT Act, Republican-led DATA Act and No TikTok on United States Devices Act would all modify IEEPA and empower the executive branch to restrict foreign technologies.

These pre-existing frameworks to regulate foreign influence in the U.S. could be repurposed to apply more specifically to social media companies, as explained in the "Policy Proposal" section below.

U.S. FRAMEWORKS REGULATING LIABILITY, PRIVACY, AND TRANSPARENCY

In the United States, much of the federal-level the debate on the regulation of social media has centered around Section 230 of the Communications Decency Act of 1996. Section 230 essentially shields social media companies from liability for illegal content posted by their users, stating that companies should not be treated as "publishers" of social media content. In doing so, Section 230 also shields social media companies from

liability for many of the harms outlined in this article, including misinformation, addictive effects, dangerous trends, and body-image issues.

Crucially, Section 230 protects social media platforms from liability even if they engage in editorial content-moderation decisions. In 2018, however, the Fight Online Sex Trafficking Act carved out an exception in Section 230 for websites that facilitate sex trafficking, which free speech advocates saw as the first step in a weakening of Section 230's overall liability protections.

There is significant debate over whether it is time to overhaul Section 230 more thoroughly. Many Republicans argue that the liability exemption is used as cover for anti-conservative content moderation by social media companies. For their part, many Democrats argue that social media companies should face more liability for not removing harmful posts. The Supreme Court is currently considering a challenge to Section 230's coverage of social media's content algorithms, raising the possibility of serious disruption if it is struck down. If the Supreme Court agrees with the lower courts that content algorithms are protected by Section 230, lawmakers may consider reform to Section 230 to specify that algorithms are not protected under this clause. This could incentivize social media companies to improve content moderation due to a fear of lawsuits, including potentially reducing the addictive effects of their algorithms or filtering mis- and dis-information, for example. However, legislative consensus on how exactly to reform Section 230 has remained elusive.

With relatively little movement at the federal level on either broad social media regulation or privacy protection, however, many states have crafted new policies in this space. California was an early leader in regulating online privacy, passing the California Online Privacy Protection Act (CalOPPA) back in 2003, mandating the posting of now-ubiquitous privacy policies. California also passed a more recent bill of privacy rights, the California Consumer Privacy Act (CCPA) of 2018. Privacy protection statutes may help reduce some of the harmful effects of social media platforms, reducing the ability of sites to track users and build detailed profiles on them, thereby mitigating the harms of potential data leaks by foreign adversaries, as well as potential political interference through algorithmic content targeting.

More recently, states have begun targeting social media algorithms and content moderation more directly. California and Minnesota have advanced bills that would aim to protect children from addictive social media algorithms, creating legal liability for social media platforms that cause addiction in California's case and banning the use of algorithms to target content to users under 18 in Minnesota's. Democrat-led states including California and New York have legislative efforts to mandate mechanisms for hate-speech reporting on social media in an effort to curb gun violence, misinformation, and bigotry. Republican-led states, led by Texas and Florida, have introduced or passed laws aimed at preventing social media companies from engaging in political censorship, thereby reducing a perceived anti-conservative bias. All of these efforts have come under criticism (and often legal challenge) for potential violation of the First Amendment. Finally, in a less controversial move, a bipartisan group of states have introduced (and in California, passed) bills that would mandate more transparency in social media content moderation decisions.

EUROPEAN UNION

The European Union has emerged as an international leader regulating social media, first with the General Data Protection Regulation (GDPR) of 2016 and most recently with the Digital Services Act and Digital Markets Act of 2022. The GDPR established the first major comprehensive privacy protection statute, covering sensitive personal and identifiable data online. Its provisions include a mandate for minimal data collection, data security regulations with fines for breaches, data storage and processing accountability rules, and data access rights for users. The GDPR applies to social media companies and is enforced by national regulators. As with California's privacy statutes, the GDPR is likely to reduce the risk of foreign data access and algorithmic targeting in social media. Importantly, the GDPR also sets the age of consent for social media use at 16, although EU member states may lower it to 13.

The Digital Markets Act (DMA) seeks to prevent large tech companies from engaging in anti-competitive behavior. One way it applies to social media companies is by preventing platforms with over 45 million active monthly users from combining user data from two dis-

tinct services the company offers (e.g., Instagram and Facebook under Meta). The act also requires these large tech firms to allow for portability of user data, both so that users are granted more control of their own data and so that the company does not have absolute control over its users' data. By limiting the market power of large social media platforms and promoting competition, the DMA may incentivize companies to do a better job of filtering misinformation or reducing other harmful health effects so that they avoid losing users to less-harmful competitors. The DMA also may restrict the granularity of personal data that may be collected, reinforcing the privacy benefits of the GDPR.

The Digital Services Act (DSA) implements more direct safeguards against social media content (rather than data) and also contains special provisions for companies with more than 45 million active monthly users.[2] This act generally maintains the exemption from liability for illegal content on online platforms, but unlike Section 230 in the United States, the law designates certain circumstances where companies can be held liable. The DSA language means that a company can be charged if it knows that there is illegal content posted on its platform but does not act to remove it. In contrast, as explained above, Section 230 provides broad immunity to tech companies from getting charged with a crime in this scenario. (There are some specific exceptions to Section 230 for copyright infringement, content related to sex work, and content that violates federal criminal law.)

The DSA also requires some transparency on companies' algorithms as well as content moderation practices. Regarding content moderation, the DSA requires that companies have "trusted flaggers" to regulate this content and report the number of actions a company takes against illegal content. The law also implements ad transparency measures, requiring that users can see who an advertisement is from and are able to report an ad if it is deemed inappropriate or violates the platform's guidelines. Companies are also required to have a point of contact within the EU that regulators may reach for accountability.

2 Facebook, Instagram, and TikTok all meet the monthly user threshold for the special provisions of the DMA and the DSA to apply.

An op-ed by Zohar Efroni at the Weizenbaum Institute for the Networked Society argued that the European laws would help prevent companies from "spreading illegal content, imposing limitations on free expression, facilitating discrimination and aggravating harms that emanate from online advertising and profiling." U.S. regulators should look to these laws and the safeguards they provide as examples of how to effectively regulate social media companies with regard to data privacy and consumer protection.

Policy Proposals

We advance here ideas for actions that can be taken both in the short and long run to address the harms of social media platforms.

SHORT-TERM ACTIONS UNDER EXISTING LAW

Given its broad authority over foreign acquisition of U.S. companies, CFIUS is in an ideal policy with which to take action in the short run. For example, in the CFIUS review of TikTok, the Committee could impose mitigation measures, including "third-party auditing of data, source code examination, and monitoring of user data logs" by U.S. regulators—all aimed at protecting U.S. user privacy. These negotiations have been repeatedly delayed, however, as U.S. government officials remain unsatisfied that the proposed arrangement sufficiently addresses all national security concerns. Therefore, unless CFIUS-imposed mitigation measures can satisfy all national security concerns, the Committee could recommend that TikTok be completely divested from its Chinese parent by forcing a sale to a U.S. entity or to an entity from a U.S. ally.

However, critical to the question of divestment is the fate of TikTok's algorithm. TikTok's video recommendation algorithm has been central in powering TikTok's success, to a degree that has not been matched by U.S. tech giants. The algorithm's potential for manipulation by the Chinese government is also central to its security vulnerabilities, and a divestment of TikTok with continued Chinese control of the algorithm would not resolve the U.S.'s national security concerns. In addition, if di-

vestment is not accompanied by data access restrictions, American national security concerns are likely to remain unaddressed, as has been suggested by TikTok representatives themselves. While ByteDance could sell TikTok together with an older version of the algorithm to an American firm that in turn could develop a more sophisticated algorithm on its own, the Chinese government may also not allow any divestment of the TikTok algorithm for political reasons, and ByteDance may not be willing to transfer it to a third party.

Given these considerations, if ByteDance is unwilling to sell the U.S. user base together with the rights to a sufficiently advanced algorithm that can be further developed by the U.S. buyer, a complete ban is the best path forward. We recognize that this will not be politically popular, especially with younger voters. Accordingly, if a ban is to be implemented, much greater bipartisan efforts need to be undertaken to further educate the American public about the stakes involved. This is one of the few subjects, it seems, where Democrats and Republicans are largely aligned.

Beyond the TikTok case, CFIUS should use its broad powers more regularly to evaluate all future social media mergers and acquisitions by foreign entities and subsequently boost confidence that such foreign influence does not threaten U.S. national security.

NEW LEGISLATION AND REGULATORY FRAMEWORKS

In addition to working within existing legal frameworks, lawmakers could consider passing new legislation to support and strengthen data sovereignty and privacy.

To address the foreign-ownership problem when autocratic regimes are involved, the laws governing foreign acquisitions could be strengthened for social media platforms. One step would be to amend Section 310 of the Communications Act of 1934 to include social media companies, thereby limiting investment by foreign entities in social media platforms and their parent companies to a 25% stake. This would initiate a review by the FCC should a foreign entity request to acquire more than a quarter of a U.S.-based social media company.

More generally, lawmakers could require every social media company with complete or even significant partial foreign investments to be reviewed by CFIUS on national security grounds if the company handles any U.S. user data. This would ensure that all social media companies are subject to a fair level of regulatory attention and defend against not only foreign access to personal data but the dissemination of foreign government censorship or propaganda.

Regarding the broader risks social media poses, for starters, Mark MacCarthy at Brookings has argued that a dedicated federal regulator should be set up to develop specific rules for the disclosure of social media platforms' internal data to users, researchers, and the public. If the appetite for a new agency is not there, additional regulatory authority could be given to the Federal Trade Commission, which has already punished TikTok for violating children's privacy, or the authority of the Consumer Products Safety Commission could be extended to apps.

Further, there is already bipartisan agreement on allowing researchers access to internal social media company data with adequate privacy safeguards and liability protections. The Platform Accountability and Transparency Act was introduced in the Senate in late December 2022, aimed at advancing transparency through scientific research of social media moderation and algorithms. Such transparency provisions would build the knowledge base for well-targeted future social media regulation, opening up the black box of social media algorithms and helping to identify the areas in which new policies are most urgently needed.

Another key piece of new legislation that is needed is a federal data protection bill, modeled on the EU's GDPR and California's CCPA. Such a law would strengthen user protections against the harvesting and misuse of their personal data by all social media companies, while building additional legal protection against foreign storage and access of U.S. data.

Such a data protection law should incorporate a higher age of consent, such as the 16-year minimum age for data collection in the GDPR, rather than the current restrictions on children under 13 currently in COPPA. Min-

imum age limits and more stringent penalties for social media companies that violate them could incentivize the development of better age-verification procedures by those companies. This would prevent young children from being exposed to harmful content and would ensure that TikTok and other social media companies are enforcing their guidelines in a verifiable way. Lawmakers might also consider measures to help minimize the amount of time teenagers spend on social media, such as incentives for schools to disallow cell phones on school grounds.

Many experts and advocates have argued that an important step in regulating social media would be re-establishing a "duty of care" standard, which is a common law duty for businesses to "take reasonable steps" not to cause harm to users, to prevent harm to users, and prevent users from using the business to harm other users. In its current form, Section 230 of the Communications Decency Act, described in the preceding section, exempts social media firms from this duty. An amended version of Section 230 could retain liability protection only for social media firms that take reasonable steps to moderate content on their platforms, thereby incentivizing firms to self-regulate to avoid lawsuits. Such a standard is currently under consideration in the UK and is very similar to the new EU standard of conditional liability in the DSA.

In addition, the U.S. should adopt the broader reforms the EU included in its DSA and DMA, which outlined standards for data handling and content moderation to protect users and prevent anti-competitive behavior among large social media companies. This would include minimal data collection guidelines, data sharing restrictions, data portability requirements, the ability for users to report inappropriate or potentially harmful ads, and "trusted flaggers" to moderate content.

The DSA also includes "co-regulatory" provisions, which David Morar at the Digital Interest Lab argues could be implemented in the U.S. without running counter to the First Amendment. Co-regulatory provisions bring companies and independent third-parties into the regulatory process to conduct risk assessments, implement codes of conduct, and audits, each of which could help broadly minimize the harms of social media.

Additional recommendations for addressing the harms of social media platforms can be found in a 2020 report from the Forum on Information and Democracy, with 50 signatories, including major world democracies like India, the United States, Germany, the United Kingdom, France, Italy, South Korea, Argentina and Canada. The Forum convened a working group on "infodemics," aimed at the online mis- and dis-information "chaos" threatening global democracy. The report outlines 250 concrete recommendations, covering themes including transparency requirements for social media platforms, meta-regulation for content moderation, and new platform design standards.

It is important to note that developing new frameworks for social media regulation and data protection is critically important, but that the unique national security challenges of foreign-adversary-owned social media companies like TikTok would persist without government intervention to force bans or divestment.

Conclusion

The ubiquitous nature of social media in American life has brought serious concern regarding national security, data privacy, and consumer protection. The well-being of young users is directly influenced by social media and its algorithms, while a lack of data security poses a direct threat to the national security of the U.S. We have seen the consequences of unregulated social media in recent years through the national security threat TikTok poses, the adverse effect of Instagram's algorithm on teens, and a lack of transparency as to who has access to personal data from platforms like Facebook, among countless other examples. This should signal to lawmakers that action must be taken.

As new industries emerge, the U.S. has historically passed policy to check the power of companies with rapidly growing influence and protect the public against their potentially harmful practices. Regulation that promotes better practices by social media companies regarding the content they display in tandem with stricter laws to prevent foreign or outside access to user data are essential to reign in tech giants. The proposals outlined in this report could be considered and taken up by

a bipartisan group of lawmakers, who have already evidenced their strong interest in taking action on social media regulation. This would substantially strengthen the groundwork for smart, safety-oriented modern technology policy. And the most controversial step—a ban of TikTok—should not be undertaken without a major, bipartisan campaign to educate Americans, especially younger ones, of the stakes involved.

About the Program

The Center on Regulation and Markets at Brookings provides independent, non-partisan research on regulatory policy, applied broadly across microeconomic fields. It creates and promotes independent economic scholarship to inform regulatory policymaking, the regulatory process, and the efficient and equitable functioning of economic markets.

If you have questions or comments about this research, contact ESMedia@Brookings.edu.

DISCLAIMER

BROOKINGS

1775 Massachusetts Ave NW,
Washington, DC 20036
(202) 797-6000
www.brookings.edu