

**MEMORANDUM**

**TO:** Interested Parties  
**FROM:** Accountable Tech  
**RE:** Bolstering Democracy Through EU Digital Governance Reforms  
**DATE:** February 11, 2022

---

**I. Overview: Global State of Play on Tech Reform**

President Biden has not minced words in warning that “democracy itself is in peril, here at home and around the world,” citing the erosion of our consensus reality – alongside rising autocracy – as what has pushed it to the brink. While it would be naive to blame this descent on any single factor, Big Tech’s usurpation of our information ecosystem has been a unique accelerant.

These modern gatekeepers are built not to foster public good or establish common truths, but to maximize engagement and profit. Correcting course will require a comprehensive approach that includes strict regulations on the collection and use of data, new accountability measures around content moderation and amplification, bold antitrust action, and more.

Congress has made encouraging progress on bipartisan proposals to update competition laws, and key regulatory agencies like the Federal Trade Commission (FTC) are also poised to pursue bold reforms. However, the Digital Services Act (DSA) and Digital Markets Act (DMA) in the European Union – a sweeping but measured overhaul of digital governance rules that aligns squarely with democratic values and American interests – represent a singular opportunity to repair the information ecosystem before we reach a tipping point.

This memo analyzes the key elements of both the DSA and DMA, comparing each component to corollary proposals put forward by leading U.S. policymakers, many of which have bipartisan support and the backing of the White House. While European efforts to regulate American-led industries have historically – and understandably – faced fierce opposition from Washington, this package reads like an omnibus bill written by top American lawmakers. Thus, the memo argues that as trilogue negotiations continue in Brussels, the Biden administration should leverage its global leadership not to delay or dilute the EU legislation, but to help drive it forward expeditiously and in its strongest form. Such an approach represents the Biden administration’s best chance to make progress on mis/disinformation in its first term.

**II. US Influence: Current Perceptions of USG Stance on DSA/DMA**

Before examining in greater depth the substance of the DSA/DMA, it is worth reflecting on how much influence the Biden administration has – especially given Brussels’ overwhelming desire to preserve our renewed transatlantic alliance after four years of President Trump – and the ways in which perceptions of USG positions are already shaping consequential policy debates.

We have heard directly from key MEPs responsible for negotiating on behalf of the Parliament that apparent USG opposition to key elements of the DSA/DMA is a top concern as trilogues get underway. In particular, there is fear that critical measures MEPs fought to secure as the package moved through Parliament – things like increased algorithmic transparency and risk mitigation obligations for large platforms, access to data for public interest researchers, curbs on gatekeepers using self-preferencing to stifle competition and innovation, restrictions on ‘dark patterns’ deployed to trick users into consenting to greater surveillance, and more – could be on

the chopping block.

For many policymakers in Brussels, the only formal communications they've seen from the Biden administration on this package have come in the form of letters outlining a litany of grievances against both the DSA and the DMA. Even amongst European leaders known for their bombast in dismissing American interests, there is by-and-large a deep desire to avoid upsetting Washington at this tenuous moment. And in lieu of any concerted engagement from the White House, the sharp criticism leveled in these letters – which reports have [repeatedly noted](#) seem to echo Big Tech's talking points – is being read as the official USG stance. This dynamic weakens the hand of key Biden-aligned negotiators and undermines the interests of the administration.

With trilogues already underway – and industry lobbyists using the ostensible backing of the USG for cover as they seek to kill or water down the most consequential safeguards included in the DSA/DMA – time is of the essence. The Biden administration should engage as swiftly and decisively as possible to clarify their positions on the package, and presumably, their support for a slew of measures they've explicitly supported in our own country.

### **III. Analysis of DSA/DMA in Relation to U.S. Policy and Biden Agenda**

The European Union is rapidly moving forward on what promises to be the most consequential and comprehensive legislative package on platform regulation in the world: the DSA, aimed at protecting people's safety and fundamental rights online, and the DMA, aimed at restraining gatekeepers' anti-competitive behavior.

The legislation was drafted and formally put forward by the European Commission in December of 2020. By late 2021, the Council of the EU – representing the interests of of the 27 member states – had settled upon a “general approach” on both the DSA and DMA, and the European Parliament adopted their own versions of the bills shortly thereafter, thus clearing the way for so-called trilogue negotiations between the three bodies.

The legislation continues to advance at a breakneck speed; France holds the powerful rotating presidency of the Council for the first half of 2022 and has made clear that getting this package across the finish line while they have the reins is a top priority. In practice, that means before the French presidential election in April.

The DSA steers clear of speech restrictions, instead taking aim at the way platforms manipulate people and public discourse for profit without any accountability. Meanwhile, the DMA's approach to reining in Big Tech gatekeepers' monopoly abuses closely mirrors the bipartisan bills being advanced by the US Congress, and in many ways, with a lighter touch.

In short, Brussels is on the doorstep of fundamentally overhauling platforms' obligations in precisely the manner the Biden administration might hope to, were it not for Congressional dysfunction and hyperpartisan obstructionism.

As Big Tech lobbies to defeat, dilute, or delay key pillars of the legislation before passage, the administration could play a decisive role by instead signaling support for the package in its strongest form, with pinprick tweaks to preserve legitimate national interests. This is a unique opening to bolster transatlantic democracy.

#### **A. The Digital Services Act**

The DSA puts forward a sweeping set of new rules for online intermediary services operating in the EU. It seeks to better protect people and their fundamental rights online, establish powerful transparency and accountability frameworks for online platforms, and guard against deep systemic societal harms like disinformation and manipulation. And despite misleading claims being peddled by Big Tech, the bill does not curtail free speech. While other efforts around the world have attempted to restrict legal but harmful content, the DSA only seeks to ensure that what is illegal offline is also illegal online, and mandates new mechanisms for transparency and appeals of those decisions.

The obligations the DSA places on companies are proportionate to their size. Baseline requirements around transparency and terms of service apply to all intermediary services and scale up to far more comprehensive burdens placed on ‘Very Large Online Platforms’ (VLOPs), which are defined as those reaching more than 10% of Europe’s 450 million consumers.

Below is a summary of the DSA’s key pillars – as passed by the European Parliament, which strengthened key provisions to expand transparency and mitigate societal harms – along with pertinent U.S. proposals:

- **Opening Up the Black Box of Algorithms And Expanding User Choice.** The most noxious aspect of today’s dominant platforms is not the *existence* of harmful content (speech), but the algorithmic amplification and microtargeting of it to the largest, most susceptible audiences possible (reach). And most users have no idea the extent to which platforms are constantly manipulating what they see – boosting conspiracy theories and exploiting their personal vulnerabilities – to maximize engagement and profits. To limit these abuses, the DSA would require all Very Large Online Platforms to:
  - Clearly present users, in an easily comprehensible way, with the main parameters that algorithmic curation tools use to rank, prioritize, or recommend content;
  - Provide users with mechanisms to make active choices about how information is presented to them, such as altering the parameters of algorithmic ranking systems;
  - Guarantee users can easily turn off recommender systems and choose from at least one other content ranking system that is not based on data profiling; and
  - Ensure users are never subject to “dark patterns” designed to manipulate or deceive them into consenting to data profiling and recommender systems.

### **US Corollaries**

***Filter Bubble Transparency Act.*** Reintroduced by Sen. John Thune (R-SD) in June 2021 with six cosponsors (3 D, 3 R), this bill would require large online platforms that utilize user-specific data and opaque content curation algorithms to clearly notify users about said algorithms. It would also allow users to easily switch to a transparent ranking system that does not use personal data, such as a chronological feed, which platforms used just a few years ago.

***Deceptive Experiences to Online Users Reduction (DETOUR) Act.*** The bicameral, bipartisan DETOUR Act – reintroduced in December 2021 – would prohibit large online platforms

*from using deceptive user interfaces, known as “dark patterns,” to trick consumers into handing over their personal data.*

***[Daily Dot, 2021](#): FTC pledges to fight dark patterns that trick users on sites and apps***

- **Risk Assessments and Mitigation with External Audits.** Today’s dominant platforms – shielded from liability or regulatory bounds – have demonstrated little interest in mitigating the societal harms they know are driven by their core business model and product design. Instead, they engage in transparency theater, touting quarterly improvements on self-referential and unverifiable metrics. The DSA would require all Very Large Online Platforms to:
  - Conduct annual systemic risk assessments to evaluate whether their content moderation practices, recommender systems, ad delivery tools, etc. have led to harms including the spread of illegal content, the infringement of fundamental rights, or manipulation of their services to undermine public health or democracy;
  - Implement effective mitigation measures tailored to the specific systemic risks identified in the aforementioned assessments; and
  - Submit to annual independent audits to assess their compliance with due diligence obligations under the DSA, and promptly implement recommendations from said audits if the reports are not positive.

### **US Corollaries**

***Algorithmic Justice and Online Transparency Act.*** Recently introduced by Sen. Ed Markey (D-MA) and Rep. Doris Matsui (D-CA), this bill would – among other things – establish safety and effectiveness standards for algorithms, require online platforms to submit their algorithms to the FTC for review, and oblige platforms to describe to users in plain language the types of algorithmic processes they employ and the information collected to power them.

***[MLex](#): US FTC's Slaughter targets algorithmic bias for potential rulemaking***

- **Mandatory Data Sharing with Vetted Researchers and Civil Society.** The importance of requiring large online platforms to finally begin sharing data access with independent researchers – rather than relying on their unsubstantiated self-reporting – cannot be overstated. As we’ve seen with COVID and anti-vaxx disinformation, the stakes are quite literally life and death. The black box maintained by dominant platforms not only shields them from criticism, but it deprives policymakers of the capacity to identify the scope of major societal threats, let alone to study the most effective interventions. The DSA would require Very Large Online Platforms to:
  - Share direct access to data – in a manner that protects privacy and trade secrets – with Digital Services Coordinators, the European Commission, and vetted academic researchers or civil society organizations upon reasonable requests to study systemic risks, evaluate the platform’s compliance with the DSA, or otherwise advance the public good; and

- Share data related to the impact of recommender systems and other algorithmic tools, content moderation practices, ad targeting practices, complaint-handling systems, and more – all of which goes beyond the prevalence of harmful content.
  - The Parliament’s successful inclusion of “civil society organizations representing the public interest” – in addition to “vetted researchers” – was a critical and hard-fought win, as there have been well-founded fears about the academic capture of major institutions by Big Tech. A related push to include journalists did not prevail.

**US Corollaries**

***Platform Accountability and Transparency Act.*** *The bipartisan PATA, introduced by Sens. Coons (D-DE), Portman (R-OH), and Klobuchar (D-MN) would require social media companies to provide data to independent researchers whose requests were approved by the National Science Foundation and give the FTC the authority to require certain data to be made proactively available to researchers or the public on an ongoing basis, such as a comprehensive ad library with information about user targeting and engagement.*

**Surgeon General Vivek Murthy’s Advisory on Confronting Health Misinformation** *urges platforms to: “Give researchers access to useful data to properly analyze the spread and impact of misinformation. Researchers need data on what people see and hear, not just what they engage with, and what content is moderated (e.g., labeled, removed, downranked), including data on automated accounts that spread misinformation.”*

- **Curtailing Surveillance Advertising.** Upending the linchpin of Big Tech’s toxic business model is critical to tackling the myriad harms that emanate from it. Given the deep financial interest Big Tech, ad-tech, and others have in preserving the surveillance advertising industry, this had been one of the more fiercely debated planks of the DSA as it moved through parliament. But thanks in part to the boost provided by the rollout of U.S. legislation to ban surveillance advertising on the eve of key votes, a bloc of MEPs known as the Tracking-Free Ads Coalition scored an unexpected victory on several measures to curtail surveillance advertising. While these limitations are likely to face renewed resistance from lobbyists and potentially members of the Council and/or Commission during trilogues, the text adopted by the Parliament would:
  - Fully ban all targeted advertising of minors;
  - Prohibit ad targeting based on users’ sensitive data, such as religious beliefs, sexual orientation, race, or ethnicity; and
  - Ensure all users can opt-out of surveillance advertising in a way that is no more difficult or time-consuming than consenting, and do so without access to other functionalities of the platform being disabled.

**US Corollaries**

***Banning Surveillance Advertising Act (BSAA).*** *In January, Reps. Anna Eshoo (D-CA) –*

*whose district includes much of Silicon Valley – and Sen. Cory Booker (D-NJ) – a longtime friend of Mark Zuckerberg – introduced the BSAA. It would effectively ban surveillance advertising, while preserving the use of a user’s general location for ad targeting, along with contextual and search advertising – effective ways to serve relevant ads without using surveillance and profiling.*

***President Biden’s Executive Order on Fostering Competition** urges “the FTC to establish rules on surveillance and the accumulation of data.” And, to that end, Accountable Tech recently submitted a petition to prohibit surveillance advertising as an unfair method of competition. The FTC requested public comments, which drew wide support from consumer advocates, civil rights groups, and privacy-respecting tech companies – including one helmed by the man who ran Google’s advertising division for 15 years.*

- **Notice and Action Requirements for Illegal Content.** Similar to Section 230, the DSA maintains a broad intermediary liability exemption for platforms, irrespective of their own proactive content moderation initiatives. However, it also establishes a robust regime to strike a balance between promoting the timely takedown of illegal content and ensuring that platforms aren’t incentivized to over-censor. It also gives users clarity throughout the process and mechanisms for appeal. The DSA would:
  - Require hosting service providers to, upon notification of ostensibly illegal content on their service, swiftly review the claims and, if appropriate, remove the posts and clearly explain the specific decision to the user;
  - Require online platforms to establish a “Trusted Flaggers” program whereby vetted independent partners with relevant expertise and competence can submit notices that are prioritized and reviewed without delay;
  - Require online platforms to establish an internal complaint-handling system for users to appeal moderation decisions and partake in an out-of-court dispute settlement for those users whose complaints could not be resolved internally; and
  - Require intermediary service providers to file annual transparency reports on content moderation actions taken at the behest of member states, removals prompted by user flags of both illegal content and violations of terms and services, actions carried out proactively, and data on complaint-handling cases.

**US Corollary**

***Platform Accountability and Consumer Transparency (PACT) Act.*** Led by Sens. Schatz (D-HI) and Thune (R-SD), the PACT Act would require large online platforms to establish a complaint system that processes reports and notifies users of moderation decisions within 21 days, to remove court-determined illegal content and activity within four days, and to produce a biannual report that includes disaggregated statistics on content that has been removed, demonetized, or deprioritized.

**B. The Digital Markets Act**

The DMA puts forward a robust, but measured, series of “do’s” and “don’ts” that are designed to rein in some of the most egregious abuses of monopoly power deployed by gatekeeper platforms to entrench their dominance at the expense of consumers, competition, and innovation.

The precise thresholds used to define platforms as gatekeepers remains a subject of significant debate, as the Parliament adopted text narrowing the Commission’s proposed scope to include only the very largest platforms.

While this has prompted claims that the DMA is anti-American, it must be noted that the bipartisan antitrust package advanced by the U.S. House Judiciary Committee was explicitly designed with thresholds meant to target four American companies (Apple, Amazon, Facebook, and Google) as those companies have maintained and abused unrivaled monopoly power over the entire digital economy for years. Moreover, these bills are all written such that any platform that becomes dominant – be they American, European, or Chinese – will be subject to the same rules after they cross these thresholds.

The key elements of the DMA track closely with the bipartisan, bicameral, White House-backed antitrust proposals moving through the U.S. Congress. Both Brussels and Washington are taking aim squarely at gatekeepers’ use of self-preferencing and app store monopolies, with further overlap on efforts to mandate increased interoperability, curb anticompetitive mergers, and more. Notably, the DMA stops far short of the most aggressive bipartisan bills advanced by House Judiciary, which would effectively prohibit covered platforms from owning other business lines that create conflicts of interest or acquiring any company with potential to become a competitor.

Below is a summary of the DMA’s key pillars – as passed by the European Parliament in a stunning 642-8 vote – along with pertinent U.S. proposals:

- **Prohibiting Gatekeepers From Self-Preferencing.** At the core of the DMA is a common-sense principle: The world’s most dominant platforms – which now serve as the global gatekeepers of information, communications, and commerce – should not be allowed to rig the vast marketplaces they control to favor their own products and further entrench their monopoly power. The DMA takes aim at this practice by prohibiting self-preferencing. Examples would be Google prioritizing its own services within its search results, or Amazon strategically surfacing its own products ahead of competitors. In particular, the DMA would prohibit gatekeepers from:
  - Giving differentiated or preferential treatment in the ranking, prominence, or display of products or services offered by the gatekeeper or businesses it controls as compared to those from other providers;
  - Restricting business users from offering customers goods or services under more favorable conditions through alternative intermediary services than those operated by the gatekeeper;
  - Leveraging their core platform services to gain unfair competitive advantages for ancillary services in adjacent markets, such as retailing or distribution activities;
  - Using non-public data from business users – or combining users’ personal data from across different sources – to gain unfair competitive advantages.

**US Corollaries**

***The American Innovation and Choice Online Act.*** *The AICO – which recently sailed through the Senate Judiciary Committee on an overwhelming 16-6 vote – and the bipartisan companion bill led by Reps. Cicilline (D-RI) and Buck (R-CO) that had already advanced convincingly through House Judiciary last June, would prevent gatekeeper platforms from rigging the marketplaces they operate. It would prohibit dominant firms like Amazon, Apple, Google, and Facebook from unfairly boosting their own products and those of key business partners or kneecapping competitors and nascent rivals to entrench their monopoly power.*

**President Biden’s Executive Order on Fostering Competition** takes aim at “Big Tech platforms unfairly competing with small businesses: The large platforms’ power gives them unfair opportunities to get a leg up on the small businesses that rely on them to reach customers. For example, companies that run dominant online retail marketplaces can see how small businesses’ products sell and then use the data to launch their own competing products. Because they run the platform, they can also display their own copycat products more prominently than the small businesses’ products.”

- **Reining In App Store Monopolies.** In addition to its broader prohibitions against self-preferencing, the DMA includes distinct provisions designed to free app developers and consumers alike from monopoly abuses of app store operators and other similar walled garden ecosystems that gatekeepers build by vertically integrating various core platform services. Specifically, the DMA would require gatekeepers to:
  - Refrain from erecting any technical barriers to prevent or discourage customers from switching to different software applications or services than those provided by the gatekeeper;
  - Prompt users where relevant to determine whether a downloaded application or app store should become the default, and enable users to uninstall any pre-installed software that’s not essential to core functionality; and
  - Allow users to install and effectively use third-party applications and app stores outside the operating systems or hardware they provide, with an exception for gatekeepers to prohibit downloads that would endanger the integrity of their products, if such measures are necessary and justified.
    - Despite this explicit allowance for legitimate security safeguards, Apple continues to assert – exactly as they have around U.S. antitrust bills – that by allowing third-party applications and app stores (or “sideloading”), the DMA would unleash an unpreventable torrent of malware attacks on users. This is purely self-interested, as Apple earns billions annually by requiring iOS users to exclusively purchase apps through its App Store, where Apple exacts 30% monopoly fees. Under the DMA, no user would ever be required to download apps from outside the App Store, and Apple already allows sideloading on macOS devices, openly [boasting](#) that thanks to their security review protocols, “Now apps from both the App Store and the internet can be installed worry-free.”



**US Corollaries**

***The Open App Markets Act.*** In August 2021, the Open App Markets Act was introduced in the House and the Senate as part of a larger effort to limit the power of Big Tech. In early February 2022, it was passed by the Senate Judiciary Committee in a 20-2 vote. The Open App Markets Act would prohibit app store companies with more than 50 million U.S. users from self-preferencing their own apps in search results, using non-public information from third-party apps to build their own similar products or services, or requiring app developers to use the app store companies' own payment system as a condition of being listed in the store. In addition, it would allow app developers to communicate directly with users and set lower prices on competing app stores.

- **Temporarily Halting Killer Acquisitions.** In some cases, the acquisition of a nascent firm triggers the loss of not only a competitive constraint, but also a product (just like when a retail acquisition results in a store closure). Such cases have been labeled “killer acquisitions” because the acquiring firm’s [strategy](#) is “to discontinue the development of the targets’ innovation projects and pre-empt future competition.” Under the DMA, the Commission would be empowered to:
  - Temporarily prohibit digital gatekeepers from engaging in acquisitions of other digital firms or those in related sectors as necessary to prevent further harms to competition in these markets;
  - Impose additional behavioral or structural remedies on gatekeepers that engage in systematic non-compliance to continue expanding their monopoly power;

**US Corollaries**

***The Platform Competition and Opportunity Act.*** This bill led by Reps. Jeffries (D-NY) and Buck (R-CO), which was voted out of the House Judiciary Committee – and the bipartisan companion bill introduced by Sens. Klobuchar (D-MN) and Cotton (R-AR) – effectively prohibits dominant digital platforms from buying up companies unless they can affirmatively prove that the acquisition would not reinforce its market position or data advantages, nor would it neutralize a potential competitor.

**[President Biden’s Executive Order on Fostering Competition](#)** announced “an Administration policy of greater scrutiny of mergers, especially by dominant internet platforms, with particular attention to the acquisition of nascent competitors, serial mergers, the accumulation of data, competition by ‘free’ products, and the effect on user privacy.”

- **Interoperability And Data Portability.** Digital markets tend to have significant network effects and are thus prone to “tipping,” whereby early competition is for the entirety of the market. Once these dominant firms establish gatekeeper status, many erect artificial barriers to entry and ratchet up switching costs to further lock-in users. Thus, a critical component to unleashing competition, innovation, and true consumer choice is to empower consumers to leave dominant platforms without losing their data and social graphs (portability) or their ability to interact with people on those platforms (interoperability). Just like Verizon phone owners can call AT&T owners without impediments, Snapchat users should be able to message friends on Facebook. As such, the DMA would require gatekeepers to:

- Implement interoperability (i.e. allow business users and providers of ancillary services to access and interoperate with the gatekeeper);
- Refrain from imposing some bundling and tying practices on business or end-users (e.g. prevent gatekeepers from requiring business users to use, offer or interoperate with gatekeeper services);
- Allow business users to promote offers and conclude contracts with end users – and end users to access content – regardless of whether they use the gatekeepers' core platform services; and
- Provide business users with continuous and real-time data portability between platforms (i.e. for data generated by both business and end users in the context of the use of the core platform services).

### **US Corollaries**

***The Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act.*** *The bipartisan ACCESS Act, which advanced through House Judiciary last June, aims to lower barriers to entry and switching costs for businesses and consumers through interoperability and data portability requirements. The measure requires a covered platform to maintain a set of transparent, third-party-accessible interfaces, including application programming interfaces (APIs), to enable the secure transfer of data to a user or to a business at the user's direction in a "structured, commonly used, and machine-readable format" and facilitate interoperability with a competing business. The ACCESS Act also gives the FTC new authorities to swiftly challenge abusive conduct that violates these interoperability and portability requirements.*

### **C. Additional Flashpoints in USG Positioning on DSA/DMA.**

As outlined in previous sections, there has been concern amongst both the U.S. advocacy community and key allies in Europe about the extent to which certain recommendations from the USG have seemed to align more closely with Big Tech's corporate interests than the Biden administration's agenda. Below are a few other specific points of consternation:

- **Compliance Delay.** In multiple letters sent to EU leaders, the USG has pushed to significantly delay compliance periods set forth in these bills. For example, while the European Commission's proposal stated platforms would be bound by the DSA's terms three months after its entry into force, a USG letter recommended "a compliance timeline of at least 18 months." The letter offered no substantive rationale as to why such a drastic extension was necessary. Given the rapid deterioration of the information ecosystem and the urgency of the digital threats to democracy, it's difficult to understand why the administration would lobby to preserve the broken status quo into 2024.
- **Ex-Ante Regulatory Enforcement Challenges:** Letters from the USG have pushed Brussels to codify in the DMA a process that effectively prohibits the EU from taking enforcement actions against gatekeepers in violation of its terms until after the company is afforded the opportunity to engage in direct "regulatory dialogues" with the Commission. Affording companies the opportunity to contest an enforcement action

before it takes effect, as opposed to challenging that decision ex-post, would significantly curtail the Commission’s ability to limit ongoing and significant harms. Indeed, a major justification for the DMA is that Big Tech companies have used lengthy antitrust proceedings to avoid accountability. As the Brookings Institution [wrote](#), the DMA “will allow European competition enforcers to cut short lengthy proceedings against the largest tech companies and instead ensure minimum conditions in important concentrated markets for more competition to become possible.”

- **Intellectual Property.** While it is proper to ensure the package protects sensitive information, there are fears the USG has been overly credulous in echoing disingenuous warnings from Big Tech about threats to IP and data security. Indeed, an industry-driven effort to include a sweeping “trade secrets” exemption in the DSA was beaten back by a broad coalition who recognized it as a trojan horse meant to negate the bill’s core transparency and accountability mechanisms.

#### **IV. Conclusion**

We are at a global inflection point. In the U.S., election disinformation and political sectarianism continue to accelerate. In India, viral calls for anti-Muslim violence have pushed the world’s largest democracy to the [precipice of genocide](#). And in Ukraine and beyond, Russia is waging modern information warfare to demoralize and destabilize the West.

It would be naive to blame Big Tech platforms alone for this cacophony of simmering fires – but around the globe, they are fanning the flames. Democracy is indeed in peril; the margin between triumph and tragedy will be narrow, and so too is the window to influence the outcome.

We have a singular opportunity: Europe is on the brink of rewriting the rules of the digital world in line with our shared democratic values. The Biden administration should leverage its global leadership to help drive the strongest possible version of this historic package across the finish line in short order, and prove that democracy delivers.