+accountabletech

MEMORANDUM

TO: Interested Parties
FROM: Accountable Tech
RE: Global Implications of EU Digital Reforms
DATE: April 26, 2022

I. Overview

On April 23, 2022, the European Union (EU) reached a deal on the Digital Services Act (DSA) – a sweeping overhaul of rules governing online intermediaries, including landmark transparency, accountability, and risk mitigation obligations for the largest online platforms. The previous month, EU negotiators secured an agreement on the DSA's companion bill, the Digital Markets Act (DMA), which takes aim at anticompetitive practices by dominant gatekeepers.

While Big Tech and its allies have painted the DSA and DMA as European attacks on Silicon Valley, the legislation reads more like an omnibus of various proposals with bipartisan support in Washington. The package creates new leverage for US policymakers to demand similar protections for American consumers and entrepreneurs, while also underscoring the fact that in lieu of swift Congressional action, the rules of the digital world will continue to be written without us.

This memo outlines key provisions of the DSA and DMA, and compares them to pertinent pieces of legislation before Congress for additional context.

II. The Digital Services Act (DSA)

The DSA sets out to protect people's fundamental rights online, and foster a safer and more accountable internet. It accomplishes this not by restricting speech, but by establishing asymmetric obligations for digital services proportionate to their size, role, and impact on the online ecosystem. While all intermediaries must meet basic requirements – like publishing clear terms of service and responding to court orders to remove pieces of illegal content – the largest online platforms must also assess and mitigate systemic harms inherent to their products, share access to data with researchers, open up black box algorithms, and more.

The European Commission will oversee these so-called 'Very Large Online Platforms' (VLOPs) and can levy fines of up to 6% of their annual revenue for noncompliance. Importantly, the threshold for VLOPs – 45 million EU users – is expected to sweep up not only American tech giants, but also dominant Chinese and European players, like Tiktok and Spotify.

Below is a summary of the DSA's key pillars and relevant US corollaries:

- **Risk Assessments and Mitigation with Independent Auditing.** The requirement for VLOPs to assess and mitigate risks inherent to their services – subject to independent auditing – may be the DSA's most important feature. It will hold tech giants accountable for the extent to which things like their core business model, product design, content policies, data practices, and ad targeting drive societal harms. Specifically, VLOPs must:
    - Conduct annual risk assessments to evaluate systemic risks of their services,

including harms to minors and other vulnerable groups, mental health, human rights, democracy, etc. and implement mitigation measures to address them;

- Submit to annual independent audits to assess compliance with due diligence obligations under the DSA, and swiftly implement recommendations; and

- Establish crisis protocols to prepare proactively for extraordinary circumstances, such as a global pandemic or an unjustifiable war against a sovereign nation.

> ***US Corollary:*** *The bipartisan **Kids Online Safety Act** – introduced by Sens. Blumenthal (D-CT) and Blackburn (R-TN) – would require covered platforms to publish annual reports assessing systemic risks to minors and mitigation tools based on independent auditing, among other protections.*

- **Access to Data for Researchers and Civil Society.** From COVID conspiracism to Kremlin propaganda, the proliferation of harmful online disinformation is killing people, yet only the platforms themselves know the scope and shape of the problem – and they have a vested interest in keeping it that way. The DSA will finally give researchers and NGOs access to the data necessary to counter deadly lies by requiring VLOPs to:

  - Share access to data – upon reasonable request, in a manner that protects privacy and trade secrets – with designated EU authorities, vetted researchers, or civil society organizations in service of the public interest; and

  - Ensure researchers can specifically study how platforms' algorithms and other systems influence the reach and salience of harmful content and actors.

> ***US Corollary:*** *Sens. Coons (D-DE), Portman (R-OH), and Klobuchar (D-MN)'s **Platform Accountability and Transparency Act** would require large social media platforms to provide vetted researches access to data for NSF-approved projects, and empower the FTC to mandate certain information to be made proactively available on an ongoing basis. (i.e. – a comprehensive ad library with data on targeting and user engagement.)*

- **Algorithmic Transparency and User Choice.** Big Tech platforms are incentivized to maximize engagement above all else, so they employ powerful algorithms to predict what content is most likely to keep each user clicking and serve it up accordingly – often without our awareness or consent. To limit these abuses, the DSA will require VLOPs to:

  - Clearly present users, in an easily comprehensible way, with the main parameters that algorithmic curation tools use to rank, prioritize, or recommend content;

  - 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

  - Refrain from deploying 'dark patterns' designed to deceive users into accepting

more invasive data profiling or otherwise depriving them of informed consent.

> ***US Corollary:*** *The bipartisan* ***Filter Bubble Transparency Act*** *would require large online platforms that utilize user-specific data and automated content curation systems to clearly notify users about the use of those algorithms, and allow users to easily switch to a transparent ranking system not based on profiling, such as a chronological feed.*

- **Banning Surveillance Advertising Aimed at Minors or Using Sensitive Data.** Upending Big Tech's business model is critical to tackling the myriad harms it motivates. The DSA takes direct aim at the most invasive forms of surveillance advertising by:
    - Fully banning targeted advertising to minors;
    - Prohibiting ad targeting based on users' sensitive data, such as religious beliefs, sexual orientation, race, or ethnicity; and
    - Requiring that platforms allow users to opt-out of surveillance advertising in a way that is no more difficult or time-consuming than consenting.

> ***US Corollary:*** *Sen. Markey (D-MA) and Sen. Cassidy (R-LA)'s* ***'COPPA 2.0'*** *bill would ban targeted ads to kids, while the bicameral* ***Banning Surveillance Advertising Act*** *would prohibit the practice altogether.*

- **Ensuring What's Illegal Offline is Illegal Online.** While the DSA maintains broad intermediary liability exemptions similar to Section 230, it establishes a regime to strike a balance between promoting the timely takedown of explicitly illegal content and ensuring that platforms aren't incentivized to over-censor. It also gives users clarity throughout the process and mechanisms for appeal. Specifically, the DSA would:
    - Mandate that companies swiftly review notifications of ostensibly illegal content, remove posts as appropriate, and clearly explain the specific decision to the user;
    - Require platforms to establish a 'Trusted Flaggers' program for experts to submit violation reports for expedited review and an internal complaint-handling system for users to appeal moderation decisions with out-of-court remediation; and
    - Require intermediary service providers to file annual transparency reports on the impetus, nature, and scope of content moderation actions taken

> ***US Corollary:*** *Sens. Schatz (D-HI) and Thune (R-SD)'s* ***PACT Act*** *would require large online platforms to remove court-determined illegal content and activity within four days; establish a complaint system that processes reports and notifies users of moderation decisions within 21 days; and produce a biannual transparency report on content moderation actions.*

III. The Digital Markets Act (DMA)

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.

To be designated as a 'gatekeeper' under the DMA, companies must have had upwards of €7.5B in annual revenue for each of the last three years or a market cap of over €75B in the last year, plus at least 45 million end users and 10,000 business users in the EU. Contrary to criticism that the bill unfairly targets only American companies, the thresholds are set to capture other firms, like Chinese e-commerce giant Alibaba and Dutch travel agency Booking.com. Gatekeepers that violate these rules can face fines of up to 10% of their annual revenue, climbing to 20% and/or structural remedies in the case of egregious systemic noncompliance.

The key elements of the DMA track closely with bipartisan, bicameral antitrust proposals moving through the Congress. Both Brussels and Washington take aim squarely at gatekeepers' use of self-preferencing and app store monopolies, with further overlap on efforts to expand interoperability, curb anticompetitive mergers, and more. Notably, the DMA stops far short of the most aggressive bipartisan bills advanced by the House Judiciary Committee in July, which would effectively prohibit operators of covered platforms from owning business lines that may create conflicts of interest or from acquiring any company that could become a competitor.

Below is a summary of the DSA's key pillars and relevant US corollaries:

- **Prohibiting Gatekeepers from Rigging Marketplaces in their Own Favor.** At the core of the DMA is a common-sense principle: The world's largest platforms should not be allowed to rig the markets they operate to further entrench their monopoly power.
    - ***Gatekeepers cannot favor their own products or services by:***
        - Giving differentiated or preferential treatment in the ranking or display of its own services than those from other providers;
        - Restricting business users from offering customers better deals through alternative intermediary services than those operated by the gatekeeper;
        - Unfairly bundling products or services across business lines, or leveraging core platform services to gain anticompetitive advantages for ancillary services in adjacent markets, such as retailing or distribution; and
        - Pre-installing or defaulting users into their own non-essential software, or preventing users from uninstalling apps.
    - ***Gatekeepers cannot engage in anticompetitive data abuses, such as:***
        - Combining user data across business lines to build comprehensive profiles for the purposes of surveillance advertising;
        - Exploiting business user data to gain unfair advantages, i.e. Amazon

scooping data from third-party sellers to launch competing products; and

- Blocking companies' ability to fully access their own data generated through business or activity on the gatekeepers' platforms.

> ***US Corollary:*** *The bipartisan* ***American Innovation and Choice Online Act*** *– versions of which have now advanced convincingly out of both the House and Senate Judiciary Committees – outlines a set of new rules to curtail dominant tech platforms from rigging the marketplaces they operate to entrench their monopoly power. It would prohibit these gatekeepers from unfairly boosting their own products or kneecapping rivals; exploiting nonpublic data or hindering businesses access to their own data; conditioning access or placement on the use of services not intrinsic to the covered platform; or preventing users from app uninstalls.*

Reining In App Store Monopolies. In addition to its broader self-preferencing prohibitions, the DMA includes distinct provisions designed to free app developers and consumers alike from monopoly abuses of app store operators. Specifically, the DMA would require gatekeepers to:

- Allow users to download and effectively use third-party applications and app stores outside the operating systems or hardware they provide;
- Prompt users where relevant to determine whether a downloaded application or app store should become the default; and
- Refrain from conditioning developers' app store access on the use of payment services.

> ***US Corollary:*** *The bipartisan* ***Open App Markets Act****, which sailed through committee with a 20-2 vote, would require operators of dominant app stores to allow users to install third-party apps and app stores from outside their walled gardens and set them as defaults. It would prohibit those gatekeepers from conditioning developers' access to app stores on the use of payment services; boosting their own apps in search results; or exploiting nonpublic data from other apps for competitive gain.*

IV. Conclusion

Taken together, the DSA and DMA amount to a comprehensive reimagining of the rules that govern the digital world. The package is not perfect – and it may not be precisely the approach Washington would have charted – but our European allies have done a tremendous service to the entire democratic world.

The package is set to be formally approved this summer and both laws should be in full force by the end of 2023. Even as the legislative window for this Congress dwindles, US policymakers have a real opportunity to leverage the EU's new roadmap to drive progress at home.