Climate Disinformation and the Digital Services Oversight and Safety Act

Summary: The draft Digital Services Oversight and Safety Act (DSOSA) bill will empower analysts and advocates working to reduce climate disinformation by requiring transparency from social media companies. Although it never uses the word "climate", climate change is, in the bill's terminology, a "systemic risk", exacerbated by disinformation and other abuses of online platforms, and therefore triggers the bill's requirements for policy documentation, transparency, and risk audits from social media companies. The lack of references to a specific topic such as climate change, or directives for content moderation itself, increases the likelihood that the provisions will pass first amendment scrutiny.

DSOSA would greatly improve climate change organizations' ability to understand climate change disinformation and will require social media platforms to provide the information articulated in Climate Action Against Disinformation's company policy recommendations.

Provisions and relevance of the bill

- DSOSA includes specific mandates for language within the community standards that line up well with a climate disinformation policy ask (p. 32).
- The bill mandates public transparency reports. The statute focuses on disclosure of aggregate statistics of content moderation, "categorized by the type of action and reason for taking the action." (p. 34) If companies have a climate disinformation policy, this should be broken out as an individual "reason" in such reports, provided a company doesn't lump together content policy violations in a manner that obfuscates their nature. Furthermore, platforms are permitted to disclose more specific data, and the bill gives broad authority to the FTC to require additional disclosures (p. 36), so there's legal room to push for specific disclosure of climate disinformation data if platforms are unwilling to subdivide within their reports.
- A lot of the most heightened obligations of the bill kick in where a "systemic risk" identified (p. 39). Systemic risk is defined generally, but includes inauthentic

behavior and amplification of content in breach of community standards where the effect can harm public health, civic discourse, public security, or the safety of vulnerable and marginalised communities (p. 20). This provides plenty of margin to push for climate disinformation to be considered a systemic risk for purposes of the statute.

- For systemic risks, platforms are obligated to document their efforts to reduce risk (p. 40) and the FTC must assess how well the platforms are doing (p. 44).

DSOSA's researcher access provisions would further help the climate advocacy community.

- The bill requires platforms to make data available to researchers through government-sanctioned programs, with ample safeguards and protection measures in place to limit the possibility of ancillary harm from arising (i.e. to prevent another Cambridge Analytica).
- One example of the information required to be made available to researchers is metrics used by the platform in their internal studies for evaluating "success and quality of content" (p. 63-64). Where platforms study climate disinfo internally, this offers the potential for broader public awareness and understanding.
- The researcher access provisions specifically permit non-university, 501c3 organization research (p. 53), which is a helpful contrast to some researcher access proposals which were limited solely to university researchers.This would allow advocates to employ legitimate research firms to bring up to date data analysis into their advocacy work.

DSOSA aligns with the European Union's Digital Services Act in meaningful ways

- Regardless of one's level of optimism regarding DSOSA, the Digital Services Act (DSA) in the European Union has been passed by the European Parliament and is widely expected to be fully adopted by the end of Q2 2022, taking effect in early 2023. The DSA is considered likely to set a global standard for platform

responsibility law, in the same way Europe's General Data Protection Regulation (GDPR) went first and changed global norms and expectations for data protection, and served to model privacy laws adopted in other countries as well as US state law including in Washington and Virginia (and in part California).

- DSOSA uses a similar framework to the DSA, imposing variable responsibilities for larger platforms and a philosophy of transparency obligations, risk assessments, and data access. This lends credibility to DSOSA, and implies that it will be a model for future American federal and state legislation, just as the GDPR shaped subsequent American privacy law.
- DSOSA uses similar language to DSA throughout, e.g. in the definition of system risk pertinent to climate disinformation:

    - ➔ [DSOSA page 20] "any malfunctioning or intentional manipulation of a hosting service, including for means of inauthentic use or coordinated, automated, or other exploitation of the service or risks inherent to the intended operation of the service, including the amplification of illegal content, and of content that is in breach of the community standard of the provider of the service and has an actual or foreseeable negative impact on the protection of public health, minors, civic discourse, electoral processes, public security, or the safety of vulnerable and marginalized communities"
    - ➔ [the Parliament's adopted Digital Services Act amendment 297, available here]: "any malfunctioning or intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service or risks inherent to the intended operation of the service, including the amplification of illegal content, of content that is in breach with their terms and conditions or any other content with an actual or foreseeable negative effect on the protection of minors and of other vulnerable groups of recipients of the service, on democratic values, media freedom, freedom of expression and civic discourse, or actual or foreseeable effects related to electoral processes and public security;"