THE EU ONCE AGAIN LEADS THE WAY IN EFFORTS TO COMBAT THREATS TO DEMOCRACY: COULD THE STRENGTHENED DISINFORMATION CODE SERVE AS A ROADMAP FOR AN ESG-STYLE SCORECARD IN THE US?

The European Union continues its efforts to counter disinformation and rein in the power of the large tech platforms; in doing so, it remains very much at the forefront of the global battle to combat disinformation (see my previous note on the ways in which that battle is evolving, available here). The latest EU effort raises interesting questions, including whether it will spur other jurisdictions to act and whether the "European approach," in its careful balancing of competing rights and interests, ultimately will yield effective results in the fight against disinformation? Could the comprehensive articulation of concepts and enumeration of tools to counter disinformation produced as part of this effort serve as a basis for measuring the progress of platforms and others in the information ecosystem for purposes of investment decisions?

On June 16, the European Commission ("EC") announced the signing of The Strengthened Code of Practice on Disinformation ("Strengthened Code") by 33 signatories, which include participants in the advertising ecosystem, advertisers, ad-tech companies, fact-checkers, emerging and established tech platforms, civil society and third-party organizations with expertise in disinformation. (*See also* EC press release, EC Policy Page and EC Q&A). This latest action comes on the heels of political agreement having been reached, first on the Digital Markets Act (in March) and then on the Digital Services Act ("DSA") (in April). (S*ee* my previous briefing note on the DSA, available here.)

The voluntary Strengthened Code builds on the Code of Practice on Disinformation published in 2018 ("2018 Code"), which was the first self-regulatory instrument adopted anywhere in the world that sought voluntary commitments from industry to counter disinformation.

In brief, the Strengthened Code brings together a more diverse range of stakeholders beyond the big platforms that were covered in 2018, empowering them to contribute to improvements in the fight against disinformation by signing up to commitments that include demonetising the dissemination of disinformation; guaranteeing transparency of political advertising; enhancing cooperation with fact-checkers; and facilitating researchers' access to data. Other enhancements over 2018, include:

- reducing with greater precision financial incentives to purveyors of disinformation;
- covering new forms of manipulative behavior;
- empowering users;
- expanding fact-checking and cooperation with fact-checkers (including coverage across member states and languages spoken in those states);
- calling for transparency around political/issue ads;
- providing better access by researchers to platform data;
- providing enhanced monitoring and reporting (including per member state and per language) – signatories will report initially (to set a baseline) within seven months, and then certain signatories will report semi-annually, others on an annual basis;
- establishing a Transparency Center to support implementation and monitor efficacy; and
- establishing a Task Force to facilitate adaptation to evolving disinformation threats.

The Strengthened Code contemplates that the envisaged Commitments and Measures will complement, and be aligned with, the requirements and objectives of the DSA and will qualify as a "code of conduct" for "Very Large Online Platforms" for purposes of Article 35 of the DSA.

The Strengthened Code applies as to each signatory to services provided by that signatory in the states of the European Economic Area.

Background

Beginning in 2015, the European Union has led the way in addressing, through legislation, a range of threats to democracy.

- In 2015, the European Council set up the East StratCom Task Force within the European External Action Service to address Russian disinformation campaigns.
- In 2016, the EC issued its Joint Framework on countering hybrid threats, and in 2018 it issued its Update on hybrid threats.
- In December 2018, the EC issued its Action Plan against Disinformation.

Most relevant to the Strengthened Code, in addition to the 2018 Code (which was preceded by a March 2018 EC Communication on Tackling Online Disinformation: A European Approach) and the Strengthened Code, we have the following:

- A public consultation, conducted during the summer of 2020, on a plan to protect European democracy (that culminated in the European Democracy Plan of Action);
- An Assessment of the Code - Achievements and areas of improvement, issued in September 2020 ("2020 Assessment");
- A European Democracy Action Plan, issued in December 2020 ("EDAP"), which identified as a priority in support of democracy, empowering citizens through four key efforts (see Fact Sheet), namely measures to:
    - ○ ***promote free and fair elections***, including legislation to ensure greater transparency around sponsored political content, revisions to rules on funding of political parties, establishment of a mechanism to counter threats to electoral processes and initiatives to harden the electoral infrastructure against threats;
    - ○ ***strengthen media freedom and pluralism***, including a Directive (proposed in April 2022) to protect against so-called SLAPPs (strategic lawsuits against public participants) and other actions to defend journalists and rights defenders (see Fact Sheet);
    - ○ ***protect journalists*** online and offline, including Recommendations (proposed in September 2021), which, among others, call for the creation of independent national support services, including helplines, legal advice, psychological support and shelters for journalists and media professionals facing threats, as well as increased protection of journalists during demonstrations, greater online safety and particular support to female journalists; and
    - ○ ***strengthen efforts to counter disinformation.***

- A COVID-19 disinformation monitoring program, set up in 2020, that invited platforms that were signatories to the 2018 Code to report on measures and tools to limit vaccine disinformation. (See June 2022 update.)
- Guidance on strengthening the Code, issued in May 2021 ("Guidance"), which was one of the action items identified in the EDAP.
- A proposed Regulation on transparency and targeting of political ads ("Political Ads Transparency Regulation"), published in November 2021.

The 2018 Code

The 2018 Code reflected an approach based on the protection of freedom of expression and other rights/freedoms guaranteed under the EU Charter of Fundamental Rights that relies, not on prohibiting or sanctioning conduct, but rather on mobilizing relevant stakeholders to commit to a voluntary regime designed to be more transparent and accountable, to make content moderation practices more transparent and to empowers citizens.

Broadly speaking, the 2018 Code set out to provide signatories with the ability to put in place voluntarily policies aimed at:

- reducing opportunities for advertising placements and economic incentives for actors that disseminate disinformation online;
- enhancing transparency of political advertising, by labelling political ads and providing searchable repositories of such ads;
- taking action against and disclosing information about malign actors' use of manipulative techniques on platform services, to artificially boost the dissemination of information online and enable certain false narratives to become viral;
- setting up technological features that give prominence to trustworthy information, so that users have more instruments and tools to critically assess content they access online; and
- engaging in collaborative activities with fact-checkers and the research community, including media literacy initiatives.

Lessons Learned

The Strengthened Code is intended to address shortcomings of the 2018 Code identified in the 2020 Assessment, as well as lessons learned from the COVID-19 "infodemic" and the deluge of disinformation relating to the war in Ukraine (more on that below). Those shortcomings identified in 2020 Assessment included:

- inconsistent and incomplete application of the 2018 Code across platforms and member states (including inconsistent implementation of restrictions on ad placements; lack of transparency around political/issue ads; lack of transparency around integrity of service; and failings around empowering users);
- a lack of uniform definitions;
- gaps in the coverage of the 2018 Code's commitments;
- a lack of appropriate monitoring mechanisms, including key performance indicators;
- a lack of commitment on access to platform data for research on disinformation (including across member states and languages spoken in those states);

- a lack of cooperation with fact-checkers (including across member states and languages spoken in those states); and
- limitations inherent in self-regulation, including limited participation from stakeholders, in particular from the advertising sector, as well as an absence of mechanisms for oversight, monitoring and enforcement, as well as reporting.

The 2021 EC Guidance

The 2020 assessment was followed in 2021 by the detailed guidance on how the Code should be strengthened by the signatories to create a more transparent, safe and trustworthy online environment.

One element of the lessons learned from the pandemic was the need to broaden the scope beyond "disinformation," narrowly defined, to pick up misinformation, though limited to appropriate circumstances so as to mitigate risks where there is a significant dimension of public harm, without unduly burdening freedom of speech.

For purposes of the Guidance, disinformation covers disinformation in the narrow sense, as well as misinformation, information influence operations (namely, coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in combination with disinformation) and foreign interference in the information space (namely, coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents).

The Guidance called for reinforcing the 2018 Code in the following areas:

- ***Broader participation***, beyond the established platforms, to encompass emerging platforms, online services that disseminate information to the public, private messaging platforms, more stakeholders from the advertising ecosystem (beyond European and national associations, to include brands, ad exchanges, ad-tech providers and communications agencies) and other players that may be at risk of monetizing disinformation (*e.g.*, e-payment, services, e-commerce platforms and crowdfunding systems).

- ***Commitments tailored to the diversity of services and roles played in the ecosystem***, corresponding to the size and nature of the services provided, with minimal opt-outs for commitments relevant to the services delivered and justifications (as contemplated by Recital 68 of the DSA).

- ***Better demonetising of disinformation***, based on more effective exchanges of information on rejected ads, improved transparency and accountability around ad placements, and de-platforming of malign actors that systematically post debunked content.

  The Guidance proposed that those participating in ad placements should identify the criteria they use to place ads, and adopt measures that enable verification of the landing/destination place of ads, with the aim of avoiding the placement of ads next to disinformation content or in places that are known for repeated publication of disinformation. Commitments should also build on and improve the availability and uptake of brand safety tools, which should integrate information and analysis from fact-checkers, researchers and other relevant stakeholders providing information (*e.g.*, on the sources of disinformation campaigns). Supported by such information and tools, brand owners and other advertisers should commit to do their utmost to avoid the placement of their advertising next to disinformation content or in places that repeatedly publish disinformation.

Cooperation among participants should be improved to exchange best practices targeting the identification of purveyors of disinformation, as well as exchange of information among platforms on rejected ads. Actions to defund disinformation should be broadened by the involvement of participants active in the online monetisation value chain.

Signatories should commit to design appropriate and tailored advertising policies that address the misuse of their advertising systems for spreading and amplifying disinformation.

The Guidance addressed political advertising and issue-based advertising separately. The Guidance noted that while there was no common definition in the 2018 Code of issue-based ads, there was a consensus that these ads would include sponsored content on societal issues or related to a debate of general interest that might have an impact on public discourse (*e.g.*, climate change, environmental issues, immigration and COVID-19). These ads should be clearly and effectively labelled and distinguishable as paid-for content, and users should be able to understand that the content displayed contains advertising related to political or societal issues. The identity of the advertiser should be visible to users.

A strengthened Code should contribute to limit or avoid risks associated with micro-targeting of individuals with political and/or issues-based advertising (including full compliance with the GDPR and other relevant laws, in particular obtaining valid consent where required).

- ***Ensuring the integrity of services***, including achieving a cross-service understanding of manipulative behavior (bots, fake accounts, account takeovers and organized manipulation campaigns) that would be prohibited, including the full range of manipulative tactics, techniques and procedures ("TTPs") that constitute impermissible "inauthentic behavior." The effort should be sufficiently broad to cover the full range of actions by which malign actors may attempt to manipulate services. The techniques identified should be sufficiently defined to enable comparisons of the prevalence of impermissible behaviors across platforms, as well as the effectiveness of actions taken to counter them.

  The effort also should provide a shared vocabulary for signatories, regulators, civil society and other stakeholders to discuss problems of online disinformation and manipulation, not only for purposes of a strengthened Code but across other forums and regimes as well, including the DSA.

  As the threat landscape is an evolving one, so too must the efforts to counter the threats. Accordingly, commitments should require signatories to address evolving manipulative techniques, such as hack-and-leak operations, account takeovers, the creation of inauthentic groups, impersonations, deepfakes, the purchase of fake engagements or the opaque involvement of influencers. A strengthened Code should establish a mechanism by which commitments can be adjusted over time based on the latest evidence on the conduct and TTPs employed by malign actors.

- ***Improving the empowerment of users***, through commitments to stronger involvement in efforts to strengthen media literacy, to enhanced risk assessments of systems and the architecture of services to reduce the spread and amplification of disinformation, and to making recommender systems transparent regarding the criteria used for prioritizing and de-prioritizing information, with the option for users to customizing ranking algorithms. Commitments should also include concrete measures to mitigate risks of recommender systems fuelling the viral spread of disinformation, such as the exclusion from the recommended content of false and/or misleading information where it has been debunked by independent fact-checkers and of webpages and actors that persistently spread disinformation. Signatories should also commit to publishing information outlining the methodology their recommender systems employ in this regard.

  Signatories should commit to provide, for all relevant EU languages, systems for the regular and consistent labelling of content identified as false or misleading and for issuing targeted warnings to users that have interacted with such content. Signatories should commit to inform users why particular content or accounts have been labelled, demoted or otherwise affected by measures taken, as well as the basis for such action.

  A strengthened Code should also contain a dedicated commitment requiring relevant signatories to offer user-friendly, effective procedures on their services, enabling users to flag disinformation with the potential to cause public or individual harm. This functionality should also support labelling systems and mechanisms to help the identification of resurging false information content already labelled as false in other languages or on other services.

- ***Increasing the coverage of fact-checking and providing increased access to data to researchers***, by offering evidence-based analysis. Relevant signatories, in particular platforms, should commit to co-creating a robust framework for access to data for research purposes. The conditions for access should be transparent, open and non-discriminatory, proportionate and justified. A strengthened Code should include a commitment to provide, wherever practicable, continuous, real-time, stable and harmonised access to anonymised, aggregate or otherwise non-personal data for research purposes through APIs or other open and accessible technical solutions allowing full exploitation of the datasets.

- ***Creating a more robust monitoring framework,*** which should be based on key performance indicators capable of measuring the implementation and effectiveness of commitments and the impact of disinformation. Two classes of indicators are relevant: service-level indicators, which measure the results and impact of the policies implemented by signatories to fulfil their commitments, and structural indicators, which measure the overall impact of disinformation in the European Union.

Tying Back to Recent Events – Fighting Propaganda with Democratic Methods

In an accompanying Joint Statement, EC Vice President Věra Jourová and Commissioner Thierry Breton called out the fact that both the pandemic and the Ukraine war have demonstrated how malign actors responsible for originating disinformation surrounding these events have gamed the online information ecosystem, often in sophisticated ways. The Joint Statement Europe emphasizes that Europe has learned its lessons and is no longer naïve. It confirms that the EC is addressing the threat in a "European way" with a combination of the DSA and the Strengthened Code. Those lessons learned are:

- Disinformation has paid off – which is why platform monetization must be halted.
- Platforms must do more – platforms do not appear to have dedicated the resources needed to fight disinformation equally in all countries and languages (*e.g.*, efforts to counter Russian disinformation in non-English speaking areas continue to be woefully inadequate); ad hoc responses to a crisis are no substitute for structural EU-cooperation with fact-checkers and content moderation teams.
- Access to data is critical and has been inadequate to date – researchers need to have access to platform data to better understand the many vectors of the threat.
- Cooperation among platforms is critical – particularly to break the cycle of amplification through coordinated use of accounts.

The EC focus on the pandemic and the Ukraine war is to be commended. We should not underestimate how effective the Russian disinformation campaigns have been, and not only in Russia, but also in Europe and in the countries in the Global South that abstained on the UN General Assembly resolution condemning Russian aggression (and now are particularly vulnerable to food insecurity, caused they believe not by Russia but by Ukraine and the West).

The Strengthened Code

The Strengthened Code sets out 44 Commitments, with each Commitment having a set of related Measures (127 in all). Signatories have signed up to the Commitments and Measures relevant to their activities, services and products via subscription documents. If Commitments and Measures are deemed not relevant or pertinent to a signatory, the signatory is to explain the reason.

Signatories that are Very Large Online Platform are to be treated differently from those that are not. The latter have the option of identifying commitments "that are relevant" to the services they provide and implementing them "through measures that are proportionate in light of the size and nature" of the services and available resources, which they can do by identifying Qualitative Reporting Elements ("QREs") and Service Level Indicators ("SLIs"). The contemplated Task Force is to "review the consistency of such adopted measures with the effective functioning" of the Strengthened Code and to adopt simplified reporting for these signatories.

Signatories have committed to implement Commitments and Measures that they have signed up to within six months. Within seven months, the Signatories are to provide the EC with baseline reports detailing how they have implemented their Commitments and provide the QRE and SLIs, as they stand one month after implementation. Signatories will be cooperating with the European Regulators Group for Audiovisual Media Services (ERGA) and the European Digital Media Observatory (EDMO), in particular in the implementation phase and in the monitoring phase of the Strengthened Code.

The Commitments and Measures that signatories embrace are addressed by category, and largely follow the Guidance:

- ***Scrutiny of ad placements (for relevant signatories – those participating in ad placement)***
  - Defund dissemination of disinformation across the advertising supply chain, and improve the policies and systems that determine the eligibility of content to be monetised, the controls for monetisation and ad placement, and the data to report on the accuracy and effectiveness of controls and services around ad placements. Relevant signatories also commit to take action to scrutinise, control and limit the placement of advertising on accounts and websites disseminating disinformation or next to disinformation content, as well as limit the dissemination of advertising containing disinformation. Strict eligibility requirements and content review should limit the ways in which disinformation can be monetised through placing ads
  - Tackle ads containing disinformation by committing to prevent misuse of ad systems to disseminate disinformation in the form of advertising messages
  - Cooperate among relevant participants that buy, sell or place digital ads, through exchanges of best practices, and extend cooperation further into the online monetization value chain to increase the effectiveness of scrutiny of ad placements of their own services
- ***Political/issue ads*** (recognizing the need to be aligned with the Political Ads Transparency Directive)
  - Adopt common definitions of "political and issue advertising" and a consistent approach across political and issue advertising; signatories also commit to clearly indicate in advertising policies the extent to which such advertising is permitted or prohibited
  - Adopt efficient labelling of political/issue ads and distinguishable as paid-for content, such that users understand that the content contains political/issue ads (including identifying the sponsor)
  - Verify commitments for sponsors/providers of ad services acting on behalf of sponsors placing political/issue ads
  - Provide user-facing transparency, including comprehensible and comprehensive information about why users are seeing a political/issue ad
  - Provide political/issue "ad repositories" and minimum functionalities for APIs to enable users and researchers to perform customized searches within the ad repositories (importantly, searches should be in as close to real time as possible and in standard formats, including on a per advertiser or candidate, per geographic area or country, per language, per keyword, per election or per other targeting criteria basis)
  - Undertake various civil society commitments
  - Collaborate through monitoring and research to understand and respond to evolving risks related to disinformation in political/issue advertising
- ***Integrity of services***
  - Develop a common understanding of mis/disinformation and of manipulative behaviors, actors and prohibited practices, including fake accounts, account takeovers and bot-driven amplification; hack-and-leak operations; impersonations; malign deep fakes; purchase of fake engagements; non-transparent paid messages

    - or promotion by influencers; creation and use of accounts as part of coordinated inauthentic behavior; and user conduct artificially amplifying reach/perceived public support for disinformation (cross-referencing the AMITT (Adversarial Misinformation and Influence Tactics and Techniques) Framework)
    - Implement transparency and obligations for signatories that develop and operate AI systems and disseminate AI-generated and manipulated content
    - Agree on cooperation and transparency in order to proactively share information about cross-platform influence operations, foreign interference in information spaces and relevant incidents that emerge on their respective services, with the aim of preventing dissemination and resurgence on other services
- ***Empowering users*** (including through efforts to dilute the visibility and spread of disinformation through improved accessibility of trustworthy content, enhancing the safe design of the architecture and enhancing efforts to enable users to detect and report false and/or misleading content)
    - Enhance media literacy and critical thinking, including for vulnerable groups
    - Roll out safe designs of architecture (to reduce viral propagation of disinformation), transparency policies (as to criteria and parameters for prioritizing or deprioritizing information) and accountability for recommender systems (including tools for assessing provenance and edit history and authenticity/accuracy of digital content)
    - Better equip users (across all member state languages) to identify disinformation (including user access to tools to assess factual accuracy through fact-checks from fact-checking organizations; warning labels from other authoritative sources), with related reporting obligations
    - Better equip users with tools to make more informed decisions when they encounter online information that may be false or misleading and facilitate user access to tools/information to assess trustworthiness of information sources
    - Provide functionality for users to flag of harmful false/misleading content (across all member state languages) that violates signatories' policies or terms of service
    - Provide a transparent appeal method for users subject to enforcement for violation of policies
    - Curb disinformation on messaging apps by building and implementing features to empower users to think critically and help them determine accuracy, without weakening encryption and with due regard for privacy
- ***Empowering the research community*** (research is tied to relevant sector-related recognized ethical and methodological best practices, which can include civil society non-profit organization; access to data is not to be extended to government bodies or law enforcement authorities)
    - Provide disclosure and access ("wherever safe and practicable") for research purposes to continuous, real-time or near real-time, searchable stable non-personal data and anonymised, aggregated, or manifestly-made public data through automated means such as APIs or other open and accessible technical solutions
    - Provide vetted researchers with access to data necessary to undertake research on disinformation by developing, funding and cooperating with an independent,

    third-party body that can vet researchers and research proposals (and co-fund the development of that body)
  - Cooperate with researchers undertaking good faith research into disinformation involving the relevant services, including having appropriate human resources to facilitate the research, and maintaining open dialogue
  - Share research that they (the signatories) conduct into influence operations and the spread of disinformation (based on transparent methodologies and ethical standards), as well as the data sets, research findings and methodologies, with the Task Force and, ultimately, the public. Research would include assessing the effectiveness of the various resilience-fostering measures (*e.g.*, labels, warnings and ex-post notifications), that are implemented
- ***Empowering fact-checkers,*** based on providing fact-checkers with automated access to actions taken regarding fact-checked content and the facts checked, and a recognition that fact-checkers need to be verifiably independent from partisan institutions and transparent in their finances, organization and methodology, and to be verified signatories of the International Fact-checking Network Code of Principles (IFCN), members of EDMO's network of fact-checkers or members of the future Code of Professional Integrity for Independent European fact-checking organizations
  - Cooperate with the fact-checking community, by establishing a framework for transparent, structured, open, financially sustainable, and non-discriminatory cooperation between them and the EU fact-checking community regarding resources and support made available to fact-checkers
  - Use, showcase and integrate fact-checking in their services, processes and contents, across all member states and languages
  - Provide access to relevant information pertinent to help fact-checkers maximize the quality and impact of fact-checking, as defined in a framework to be designed in coordination with EDMO and an elected body representative of the independent European fact-checking organisations
  - Set standards for fact-checkers
- ***Transparency Center; Task Force and Monitoring***
  - Set up and maintain a common Transparency Center website
  - Ensure that the Transparency Center has access to all the relevant information related to implementation of the Commitments and Measures, and that the information is presented in a searchable, easy-to-understand manner, per service, including, importantly, geographical and language coverage; in a crisis, signatories commit to use the Transparency Center to publish information regarding specific mitigation actions taken
  - Participate in a permanent Task Force for evolving and adapting the Strengthened Code, including by way of updating the Commitments and Measures based on technological, societal, market and legislative developments
  - Commit adequate financial and human resources, and put in place internal processes, to ensure implementation of the Commitments and Measures (including outlining the teams and processes in place, per service, to comply to achieve full coverage across member states and languages) and to provide regular reports on QREs and SLIs.

- Work with the Task Force to develop and publish Structural Indicators within nine months. Relevant signatories also commit to provide reports upon request to the EC around elections or crises
- Commit, in the case of Very Large Online Platforms, in alignment with the DSA, to be audited by independent organizations for compliance with their commitments (at their own expense)
- Commit, in the case of Very Large Online Platforms, to report every six months on implementation of Commitments and Measures they signed up to including on the relevant QREs and SLIs at the service- and member state-level; other signatories commit to report on an annual basis – reporting will be based on harmonized reporting templates to be developed with the Task Force

Link to the DSA and the Political Ads Transparency Regulation

The DSA calls for a supervised risk-based approach, obligating Very Large Online Platforms to mitigate systemic risks posed by their systems, including the spreading of illegal content as well as disinformation. A new European Board of Digital Services and direct enforcement powers delegated to the EC under the DSA are to provide oversight of the new rules. The DSA encourages the implementation of voluntary initiatives, such as "codes of conduct" (in Article 35). The DSA will impose its own set of provisions on data access and scrutiny, including by "vetted researchers" (Article 31).

According to the EU Q&A, the Strengthened Code is intended to become a mitigation measure (for purposes of Article 27 of the DSA) and a "code of conduct" (contemplated by Article 35 of the DSA) recognised under the so-called "co-regulatory framework"[1] of the DSA for Very Large Online Platforms that sign up to Commitments and Measures. In short, living up to commitments under the Strengthened Code is seen as assisting Very Large Online Platforms in mitigating risks stemming from disinformation on their services (that is, as the Joint Statement noted, the Strengthened Code "will play an important role in the assessment of whether Very Large Online Platforms have complied with their legal obligations [under the DSA] of mitigating risks stemming from disinformation spreading on their systems").

Recital 68 of the DSA provides that "[t]he refusal without proper explanations by an online platform of the [EC's] invitation to participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform has infringed the obligations laid down by [the DSA]." Recital 61 of the DSA, in the context of a discussion of required audit reports and audit opinions, notes that a positive opinion should be provided where a Very Large Online Platform "complies with its obligations under

[1] The "co-regulatory" concept is a mechanism whereby an EU legislative act entrusts attainment of defined objectives to parties recognized in the field. In the context defined by the legislative act, affected parties may conclude voluntary agreements for the purpose of determining practical arrangements – per the EU Interinstitutional agreement on better law-making. "Co-regulatory" is separate from "self-regulation."

the DSA *or, where applicable, any commitments it has undertaken pursuant to a code of conduct… .*"

There is a general view that once the DSA enters into force, in practical terms enforcement will be a function of investment by the EC and national regulators. Much remains to be seen.

The Strengthened Code complements the proposed Political Ads Transparency Regulation, through signatory-led measures to achieve progress in ensuring the transparency and public disclosure of paid-for political content. The Strengthened Code should make it easier to recognize political ads due to more efficient labelling and new transparency obligations.

Concluding Thoughts

The EU effort – embracing the European approach – is premised on a multi-stakeholder strategy. We would call it a whole-of-society approach that encompasses a continuum:

- *from* operational commitments by the platforms and other tech companies;
- *to* critically important access to data by third parties for fact-checking and research involving safe and transparent processes for anonymized data-sharing at scale;
- *to* networks of fact-checkers;
- *to* monitoring/reporting;
- *to* enhanced resilience through media literacy programs.

The Strengthened Code goes further by far than legislative efforts in any other jurisdiction (including the United States) to address the pernicious effects of mis/disinformation and the related attacks more broadly on democracy.

The new effort roughly doubles the number of signatories that signed up to the 2018 Code. There are, however, some noticeable absences from the list, including Telegram, Amazon and Apple, although the Strengthened Code remains open for signature (and signatories can also withdraw).

The EC should be congratulated for shepherding through a strengthened framework that addresses a number of recognized weaknesses of the 2018 Code (*see, e.g.* ISD Cracking the Code: An evaluation of the EU Code of Practice on Disinformation), and also addresses external factors such as the significant evolution in mis/disinformation tactics and tools now readily deployed by malign actors. It should go without saying that much has been learned since 2018.

Admittedly the EC, as a compromise in balancing rights of free speech and the existing EU legislative landscape, has decided to continue in effect to outsource compliance to the signatories. These are merely commitments. The DSA, once it enters into force, is mandatory. There is, as noted, the "co-regulatory" link between the DSA and the commitments of Very Large Online Platforms under the Strengthened Code, but to be clear this does not transform these commitments into mandatory obligations. However, Recital 68 could provide a basis for enforcement for failure to adhere to their commitments. The hope should be that the signatories, having negotiated and then signed up to commitments, will live up to those commitments.

Regrettably, the United States lags behind. European policymakers largely are united in the view that disinformation poses an existential threat to democracy and that an open democratic society depends on public debates among well-informed citizens able to express their will through a free and fair political process. In the United States, we face the same threats (perhaps even more insidious threats), and yet we seem unable to move forward in any meaningful way, while Europe lays out a roadmap that it has been refining over the past seven years. Consider the likelihood of getting buy-in on Capitol Hill for a US version of the European Democracy Action Plan (safeguarding free and fair elections?) – zero to none. Sadly, we seem equally burdened when it comes to addressing other pressing existential issues, such as climate change, through legislation.

Perhaps though, through stakeholder pressure, particularly institutional and other significant investors, we may see similar commitments extended by the signatories, and others, for the benefit of US-based users. Said another way, perhaps the Strengthened Code could provide a comprehensive blueprint for an ESG-like scorecard (suggested in a previous briefing, available here) that forms the basis for consistent, comparable, reliable and decision-useful metrics for institutional and other significant investors investing in the tech sector that wish to orient capital flows in support of democracy.

*   *   *   *

Mark S. Bergman*
7Pillars Global Insights, LLC
Washington, D.C.
June 21, 2022

*Member, Board of Trustees, Institute for Strategic Dialogue