THE FIRST TRANCHE OF OBLIGATIONS UNDER THE EU DIGITAL SERVICES ACT BECAME EFFECTIVE ON AUGUST 25TH

On Friday, the first set of obligations under the EU Digital Services Act (the "DSA") became effective. That first set of obligations applies to the 19 largest platforms designated by the European Commission (the "Commission") as very large online platforms ("VLOPs") or very large online search engines ("VLOSEs"), in each case based on their online reach (at least 45 million users in the European Union).[1] Platforms with fewer than 45 million users in the European Union will be subject to the new rules beginning February 17, 2024.

The DSA represents landmark legislation that is likely to become the global template for the regulation of social media platforms. The legislation, among other things:

- bans or limits certain user-targeting practices (including so-called "dark patterns" that manipulate users so that they are unable to make autonomous and informed choices or decisions,[2] and content aimed at minors);
- imposes requirements for platforms to ban certain content and to prevent harmful content from spreading online; and
- imposes requirements on platforms to share certain internal data with regulators regarding content moderation practices and with third-party researchers.

---

[1] The DSA entered into force in November 2022. It had direct effect in EU member states, and as such did not require transposition into national law. It also applies to the four member states of the European Free Trade Association.

The timeline called for VLOPs and VLOSEs to become subject to the DSA rules four months after they were so designated by Commission, which was on April 25. The VLOPs designated are: Alibaba AliExpress; Amazon Store; Apple AppStore; Booking.com; Facebook; Google Play; Google Maps; Google Shopping; Instagram; LinkedIn; Pinterest; Snapchat; TikTok; Twitter; Wikipedia; YouTube; and Zalando. The VLOSEs designated are: Bing and Google Search. Amazon and Zalando have challenged their designations in court.

[2] In January, the Commission released the results of an investigation of a screening of 399 retail websites that focused on three specific types of manipulative practices used to push consumers into making choices that may not be in their best interest (dark patterns), including fake countdown timers; web interfaces designed to lead consumers to purchases, subscriptions or other choices; and hidden information. The investigation found that 148 sites contained at least one of these three dark patterns.

Early versions of the DSA contemplated a ban on so-called "surveillance advertising" (the central pillar of the social media platform business model that enables the micro-targeting of ads based on profiling and tracking of search history and other online activities of individual users), but the final version applies the ban only to ads targeting minors. The dark pattern ban survived.

Next month, the designation of gatekeepers will be made under the EU Digital Markets Act, with obligations effective March 6, 2024 (*see* my March 2022 briefing note, available here) and, in the not too distant future, the EU will also have legislated curbs on AI platforms (*see* my April 2023 briefing note, available here).

As summarized in my March 2022 briefing note, the DSA applies to various categories of online service providers, with a tiered-approach to regulation, and it has extraterritorial effect, meaning it applies to platforms regardless of where they are headquartered or otherwise located, but only in respect of services or products provided in the European Union. Specifically, the DSA covers:

- **intermediary services** offering network infrastructure: internet access providers and domain name registrars, including the following:
- **hosting services** such as cloud and webhosting services, including the following:
- **online platforms** bringing together sellers and consumers such as online marketplaces, app stores, collaborative economy platforms and social media platforms; and
- "**very large platforms**," which reach at least 10% of the 450 customers in the European Union (*i.e.*, VLOPs and VLOSEs) and are deemed to pose particular risks in the dissemination of illegal content and societal harms.

In essence, the DSA (*see generally*, DSA FAQ):

- ***imposes measures to counter illegal goods, services or content online***, such as a mechanism for users to flag such content and for platforms to cooperate with "trusted flaggers";
- ***imposes new obligations on traceability of business users in online market places***, to help identify sellers of illegal goods or reasonable efforts by online market places to randomly check whether products or services have been identified as being illegal in any official database;
- ***provides for effective safeguards for users***, including the ability to challenge platforms' content moderation decisions;
- ***imposes bans on certain types of targeted advertisements on online platforms*** (*e.g.*, when they target children or when they use certain categories of personal data, such as ethnicity, political views or sexual orientation);
- ***imposes transparency measures*** for online platforms in respect of a variety of issues, including in respect of the algorithms used for recommendations;
- ***impose obligations on VLOPs and VLOSEs*** to prevent the misuse of their systems by taking risk-based action and by independent audits of their risk management systems;
- ***requires access by researchers to key data of VLOPs and VLOSEs*** in order to understand how online risks evolve; and

- ***provides for an oversight structure to address the complexity of the online space***: EU member states will have the primary role, supported by a new European Board for Digital Services; for VLOPs, supervision and enforcement will be undertaken by the European Commission.

VLOPs and VLOSEs

Beginning in April, VLOPs and VLOSEs had up to four months to comply with the full set of new obligations under the DSA, which meant adapting their systems, resources and processes for compliance, setting up an independent system of compliance and carrying out, and reporting to the Commission, their first annual risk assessment.

Essentially, the new obligations are intended to empower and protect online users, including minors, by requiring the designated services to assess and mitigate their systemic risks and to provide robust content moderation tools. This includes:

More user empowerment:

- users will get clear information on why they are recommended certain information and will have the right to opt-out from recommendation systems based on profiling;
- users will be able to report illegal content easily and platforms have to process such reports diligently;
- advertisements cannot be displayed based on the sensitive data of the user (such as ethnic origin, political opinions or sexual orientation) – this is as close as the DSA comes to addressing surveillance advertising;
- platforms need to label all ads and inform users on who is promoting them; and
- platforms need to provide an easily understandable, plain-language summary of their terms and conditions, in the languages of the member states where they operate.

Strong protection of minors:

- platforms will have to redesign their systems to ensure a high level of privacy, security and safety of minors;
- platforms will no longer be permitted to provide targeted advertising based on profiling directed at minors;
- platforms were required to provide special risk assessments, including as to negative effects on mental health of minors, four months after designation and made public at the latest a year later; and
- platforms will have to redesign their services, including their interfaces, recommender systems, and terms and conditions, to mitigate these risks.

More diligent content moderation, less disinformation:

- platforms and search engines need to take measures to address risks linked to the dissemination of illegal content online and to negative effects on freedom of expression and information;
- platforms need to have clear terms and conditions and to enforce them diligently and non-arbitrarily;
- platforms need to have a mechanism for users to flag illegal content and need to act upon notifications expeditiously; and
- platforms need to analyze their specific risks, and put in place mitigation measures – for instance, to address the spread of disinformation and inauthentic use of their service.

More transparency and accountability:

- platforms need to ensure that their risk assessments and their compliance with all the DSA obligations are externally and independently audited;
- platforms will have to give access to publicly available data to researchers; later on, a special mechanism for vetted researchers will be established;
- platforms will need to publish repositories of all the ads served on their interface; and
- platforms need to publish transparency reports on content moderation decisions and risk management.

The Financial Times reported on Friday that social media companies, including Meta, Snap and TikTok, have given millions of users the option to turn off certain personalized content, "which had been considered key to the platforms' success in hooking users." These companies, as well as Google, have also restricted targeted ads for children under 18, while providing users with more information on why they have been targeted by certain marketing. Platforms are reported to have allocated significant personnel to comply with the DSA.

Earlier this week, Meta issued a statement announcing new features and additional transparency measures for EU users in response to the DSA. The statement notes that the DSA "is a bid deal not just for European tech companies but for all tech companies that operate in the EU, and it will have a significant impact in the experiences Europeans have when they open their phones or fire up their laptops." TikTok issued a similar statement on fulfilling its commitments under the DSA earlier this month, and Snap issued its statement on its new features and transparency measures to comply with the DSA earlier this week, as did Google in its statement on complying with the DSA.

Concluding Thoughts

As summarized by the Associated Press, on Friday, platform users in the European Union woke up to five obvious changes:

- they can turn off AI-recommended videos;
- it will be easier for them to flag harmful content;
- they will know why their online posts were taken down;
- they can report online availability of counterfeit products and illegal content; and
- children under 18 will no longer see personalized and targeted ads.

Most of the affected platforms are headquartered in the United States.

Once again, the European Union has first mover advantage in shaping the legal and regulatory landscape applicable to a series of activities that so thoroughly permeate everyday life. The European Union was the first to regulate online privacy and is well ahead of other jurisdictions in imposing sustainability obligations on businesses and financial market participants (*see* my August briefing note, available here). That said, commentators are divided on whether the "Brussels Effect" (a term coined by Columbia Law School professor Anu Bradford to describe the effect of EU legislation/regulation in shaping the global business environment, and best illustrated by the impact of the GDPR on privacy legislation worldwide) will apply to the DSA and the DMA. It is early days, but it is hard to imagine the global platforms choosing to forgo the EU market on the ground that the costs are too high, particularly if US legislation moves forward in parallel.

Perhaps too, Congress will be galvanized to pass parallel legislation (as I set out in my June briefing note, available here), as there is no better representation of the public interest than protections now accorded to 450 million online users.

* * *

Mark S. Bergman
7Pillars Global Insights, LLC
Altaussee, Austria
August 27, 2023