LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
TUESDAY, OCTOBER 17, 2023

The Digital Services Act reaches the USA

By Robert Spano, Vivek Mohan, Jan Przerwa and Wesley Sze

Shutterstock

The Internet has made it possible to bring people together in new ways and make the world seem smaller than ever before. But as much as the Internet may stand for unification and integration, companies operating on the web face an increasingly fragmented and complex set of rules and regulations under which they must operate. American companies are no exception. To be sure, more than 25 years ago, Congress recognized the significant benefits that a flourishing Internet technology sector offers and paved the Internet regulatory path with Section 230 of the Communications Decency Act of 1996. *See* 47 U.S.C. § 230(a), (b). But modern day Internet regulation is coming from elsewhere - not only from states and regulators within the United States, but also from abroad.

Across the Atlantic Ocean, European regulators have attempted to further regulate the Internet by passing legislation designed to fundamentally change how companies provide services online. The European Union's regulatory reach has recently expanded with the Digital Services Act (DSA), which seeks to regulate the way online intermediary services moderate content and protect fundamental rights of their users. And U.S. companies must not bury their heads in the sand: while the DSA's regulations are formally limited to online services that have a "substantial connection" to Europe, their effects may extend far beyond those borders given the interconnectedness of the Internet and the worldwide reach of the U.S. technology sector.

Background about the DSA

The DSA might be one of the most comprehensive Internet regulation regimes enacted so far. Its general requirements will kick into effect on Feb. 17, 2024. The DSA applies to all Internet intermediary services which either have an establishment in the European Union (including subsidiaries), or which offer services that have a "substantial connection" to the European Union (assessed on case-by-case basis).

Unlike Section 230, which generally grants broad immunity to online services from being legally responsible for third-party content, the DSA introduces a somewhat stricter liability regime that exempts services from civil liability for third-party content under more limited conditions than its U.S. counterpart. And the DSA goes much further than that. While it does not require providers to actively monitor content on their services, the DSA imposes prescriptive requirements on the design of content moderation processes, like obliging providers to justify content takedowns and to provide access to out-of-court dispute resolution for users unhappy with their content moderation decisions. Furthermore, the DSA requires "online platforms" to provide additional information about online ads, and bans targeted ads based on profiling using sensitive data such as political opinions, religious beliefs or sexual orientation. The DSA also features a set of strict rules for marketplaces regarding traceability of merchants and rights to information for customers who bought an illegal product.

The DSA goes even further for "very large online platforms" (VLOPs), which are online services with more than 45 million average monthly active recipients. So far, the European Union has desig-

nated 19 services as "VLOPs" that must comply with this special regime, and more designations may be on the way. *See* https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413. The system is conceptually based on the European Union's financial system supervision, with a central regulator overseeing the largest companies. At the core of the VLOP rules is the requirement that VLOPs conduct a self-assessment of the "systemic" risks on their services and take mitigating measures for the identified risks. Those assessments will be subject to a third-party audit. Additionally, the DSA imposes a handful of additional requirements on VLOPs, such as to create public ad libraries, allow users to opt-out from recommender algorithms, and grant data access to vetted researchers. Noncompliance risks hefty fines of up to 6% of global turnover. These special requirements for VLOPs went into force in August 2023.

The new regulations, in particular the VLOP rules, are far-reaching and often go to the heart of how intermediary services design and implement their core technologies and user experience. In compliance efforts, we are already seeing some companies taking measures going beyond the European Union and making changes at a global level. This may very well become yet another example of the "Brussels Effect" - and make the DSA a *de facto* standard in other jurisdictions, like it was with the GDPR.

What this means for U.S. companies

While formally limited to the European Union, the DSA has global implications, and any company whose services have a "substantial connection" with Europe ought to take notice. The standard suggests something more than merely being able to access a website from Europe, and can be met by either having a "significant" number of users in one or more of the European Union countries or "targeting" such users (e.g., having a top-level domain associated with a European Union country or offering the ability to order products or receive customer service in a local language).

For now, the DSA's most burdensome obligations are only being imposed on VLOPs - the majority of which are based in the United States. Consequently, many of the country's largest technology companies that have been designated as VLOPs are already keenly aware of these requirements. But companies that have not yet seen the eye of the European Union's regulatory bureaucracy should take stock of their services, determine the scope of their European exposure, and get ready for the Feb. 17, 2024 deadline, which is when the DSA's general regulations go into effect for all online services.

Moreover, the DSA raises important questions about how Internet regulation in other jurisdictions interact with U.S. policies and regulatory approaches. The DSA is just the latest example of regulators from abroad stepping in with their own views, and it is only one of many: the European Union's Digital Markets Act is already in force and the European Union is working on the new Data and AI Acts. This changing regulatory landscape will present new challenges for U.S. technology companies that they must overcome if they are to continue being leaders and innovators.

Members of Gibson, Dunn & Crutcher LLP's Privacy, Cybersecurity and Data Innovation Practice Group, **Robert Spano** *is a partner based in London,* **Vivek Mohan** *is a partner based in Palo Alto,* **Jan Przerwa** *is an associate attorney based in Brussels, and* **Wesley Sze** *is an associate attorney based in Palo Alto.*