The Digital Services Act and Small and Medium Enterprises as users of online services

Dr Mikołaj Barczentewicz[1], Senior Lecturer in Law at the University of Surrey[2]

The proposed EU Digital Services Act (DSA) aims to protect users of digital services, but unfortunately it also creates serious new risks for both consumers and SME users. The DSA should be more mindful that national authorities will likely have limited knowledge and motivation to safeguard interests of foreigners.

The DSA gives far-reaching powers to national authorities to issue extra-territorial orders "against illegal content". It also empowers "trusted flaggers" to notify platforms about illegal content. Such flaggers will be exclusively regulated in their country of establishment. Neither of those solutions provides potentially affected users with effective redress, even in cases of ideologically motivated orders or flagging.

The DSA also attempts to increase transparency of online platforms, while forgetting about the interests of the users whose data will be subject to such transparency. In particular, the DSA risks destroying the SMEs that rely on their skill in targeting ads on large online platforms. The DSA will make their targeting criteria (e.g. keywords) public so that they can be copied for free by any competitor, including non-European ones.

Interests of SME users need more serious attention

The Digital Services Act (DSA) proposed by the EU Commission in December 2020 is an important opportunity to ensure that EU law continues to support the great economic and social benefits that Europeans enjoy from online services (Oxford Economics, 2020). However, the proposed DSA is in need of amendment. In this brief analysis, I focus on some of the ways that the DSA, if unchanged, will negatively affect small and medium-sized enterprises (SMEs) in Europe. I draw here on my previous work on the DSA.

SMEs can be both providers and users of services in the scope of the DSA. As providers, some SMEs have local ambitions, e.g. local providers of internet access or providers of website hosting services to a small number of clients. Some are startups with aspirations to grow and reach large numbers of users in Europe and beyond. However, many more European SMEs are users of digital services—e.g. 25% of all EU SMEs advertise online and as many as 44%-46% do so in Denmark, Malta, Norway and Sweden (Eurostat, 2018). The debate on the DSA should thus focus more on how regulation of *providers* will affect smaller business *users* of online platforms, not just the platforms themselves.

No "asymmetric regulation" benefit for *users* of digital services

To an extent, the DSA takes into account the interests of SME *providers* of digital services by imposing some duties only on larger online platforms (asymmetric regulation). But this does not apply to SMEs as *users* of digital services (and of large online platforms in particular). It is unrealistic to expect the interests of SME users of online platforms to be adequately protected if the DSA creates incentives for providers and regulators to take actions that may harm SME users.

National authorities may fail to safeguard lawful interests of *users* from *other* EU countries

Authorities from one EU Member State may lack sufficient motivation and knowledge to safeguard the lawful interests of SME users of digital services from *other* Member States. In particular, content that is legal in one Member State may be considered illegal in another Member State and thus users may be affected by content prohibitions coming from other countries. This is particularly salient under the DSA given (1) the extraterritorial orders against illegal content and (2) the wide-ranging powers of national "Digital Services Coordinators" ("DSCs").

[1] Dr Mikołaj Barczentewicz an academic lawyer specialising in law and technology. He is a Senior Lecturer (Associate Professor) in Law at the University of Surrey, a Research Associate at the University of Oxford and a Fellow at Stanford Law School. He holds a D.Phil. (Ph.D.) in Law, M.Phil. in Law and M.Jur. from the University of Oxford, as well as a Polish law degree from the University of Warsaw.

[2] The author's work related to this report was supported by Google. The contents of the briefing reflect the views of the author. They do not represent the views of Google or any other organisation with which the author is affiliated. Thanks for comments and input to Allied for Startups, Center for Data Innovation, Computer & Communications Industry Association (CCIA Europe), and Union of Entrepreneurs and Employers (ZPP).

The country-of-origin principle does not apply to users

The country-of-origin principle is valuable and should be retained in the DSA, but currently it only applies to providers of digital services. That is, only the providers will benefit from being regulated by the authorities of their country of establishment and not from other Member States (with the notable exception of orders against illegal content). The DSA could also give effect to the country-of-origin principle for the users of digital services, including SME users. Those two applications of the country-of-origin principle may be reconciled, for example, by making sure that DSCs of the country of establishment can only take regulatory action in respect of service providers following binding consultation with DSCs from countries where the provider in question has users. Another solution may be to give users domestic legal redress against regulatory actions by authorities from another Member State.

The risk of overblocking of user content

If a service provider will only be able to refuse to remove content provided by an SME client and reported by someone as potentially illegal if the provider devotes significant resources to an investigation or to litigation, then the provider will likely simply "overblock" (Keller, 2015; Husovec, 2021; Civil Society Joint Statement, 2021). This is particularly risky in case of providers with limited resources. As the UN Rapporteur on freedom of opinion and expression noted "such rules involve risks to freedom of expression, putting significant pressure on companies such that they may remove lawful content in a broad effort to avoid liability" (Kaye, 2018). Theoretical availability of safeguards will give way to economic calculation and this basic insight of economic analysis of law needs to be taken into account by the DSA. The notion that imposing a requirement for very large online platforms to assess "negative effects for the exercise of the fundamental rights" will mitigate this is naive in the extreme and in any case this requirement will not apply to all providers.

Below I consider the key aspects of the DSA that in practice will negatively affect SMEs.

Extraterritorial orders against illegal content

Insufficient incentives to protect the interests of law-abiding SMEs are particularly clear in the context of "orders to act against illegal content" (Article 8 DSA). The DSA will require providers to obey such orders issued by national authorities. Instead of accepting the sound principles that determinations of what constitutes illegal content can only be decided by the courts and only have effect within the boundaries of the domestic jurisdiction, the DSA allows Member States to designate "administrative authorities" with powers to issue such orders and allows for orders to have extra-territorial scope. This practically guarantees that national administrative agencies will apply their restrictive national rules on speech and demand removal of content in other EU Member States, even if such demands are illegal in some other countries. Such demands may violate the safeguards provided by the DSA (Article 6(2)(a) and (b) and recital 31), but the very considerable cost of resisting an unlawful, but perhaps not manifestly unlawful, order will be entirely on the providers and they will often simply acquiesce services (Oxford Economics, 2020; Eurostat, 2018). Elsewhere I proposed a solution involving a right for users affected by an Article 8 order to request scrutiny and binding remedial action by their domestic Digital Service Coordinator, irrespective of where the order originated.

Example A

An administrative authority of one Member State may issue an order to act against:

- allegedly illegal content authored by users from other EU countries, but which is not really illegal or at least not illegal in the rest of the EU; this could affect political content (e.g. because it is considered "right wing") or content that is viewed as promoting LGBTQIA+ rights;
- what they mistakenly believe are counterfeit products offered on a large online eCommerce platform by SMEs from another Member States;
- advertisements on a large online platform by SMEs from another Member State, which allegedly constitute unfair commercial practice, but only according to an idiosyncratic legal interpretation adopted in the Member State of the authority issuing the order.

The platform may rationally not want to shoulder the cost of litigating against such an order. The affected SME users of the platform will not be able to get a remedy from their domestic courts and may be unable to afford the cost of fighting in the courts of the Member State which issued the order.

Trusted flaggers

Digital Services Coordinators will have the power to grant the special status of a "trusted flagger" to organisations, including industry bodies that represent narrow interests of specific enterprises (Article 19). Online platforms, and especially very large online platforms, will have a duty to prioritise consideration of notices of allegedly illegal content submitted by trusted flaggers. The status of a trusted flagger will be conferred by the DSC of the Member State where the would-be flagger is established. An authority from one Member State will have no power over a trusted flagger established in a different Member State, even if the flagger will focus on reporting content provided by users coming from the former country. The DSC that authorised a trusted flagger may have insufficient knowledge or motivation to police the flagger's non-meritorious or otherwise abusive activity harming users coming from different Member States.

Example B

Ideologically-motivated flagging: A trusted flagger from one EU country notifies online platforms about content the flagger is ideologically opposed to (e.g. because they see the content as "right wing" or as pro-LGBTQIA+) claiming that is either illegal or against providers' terms of service. Some service providers do not have the resources to investigate or to go to court in every case, hence they decide to remove much of the flagged content. When the authors of the removed content from other EU countries complain about the flagger to the only authority that can remove the "trusted flagger" status—the authority from the flagger's country—the authority ignores their concerns because it shares the ideological perspective of the flagger.

Example C

Alleged counterfeits: An EU country gives the status of a trusted flagger to an organisation representing interests of a narrow group of manufacturers. The flagger organisation sends tens of thousands of illegal content notices to providers of online marketplaces allegedly pointing to counterfeits of products of the manufacturers whose interests the flagger represents. The offers covered by the notices predominantly come from SMEs from other EU countries than the country of the trusted flagger. The notices submitted by the trusted flagger do not provide good evidence that the offered goods are counterfeit, but the marketplace providers do not have resources to investigate such high numbers of cases and they err on the side of over-removing. When the SMEs from other EU countries complain to the authority from the country of the flagger, the authority ignores their concerns because it is not motivated to protect SMEs from foreign countries.

Data access

The DSA will create a new mechanism for access to data of very large online platforms by national authorities (DSCs) and by "vetted researchers" (Article 31). There are strong privacy and security concerns about this provision. But there are also concerns about the protection of commercially sensitive data of SME users of online platforms - e.g. sellers using online marketplaces. Even though the DSA says that detailed rules on how data access would work must take into account the interests of "the recipients of the service", there is a risk that the interests of SMEs will not be adequately safeguarded in the future rule-making process.

Importantly, users of the online service—whose data will be potentially at risk—will have no say in the process of data access. Only the provider of the online platform will be able to request amendments of a data access request. But just like in cases discussed earlier—it should not be expected that the provider will have sufficient motivation or resources to make the case for the protection of user interests, as distinguished from the providers own interests. Moreover, it will be the DSC of the country where the provider of the online platform is established who will decide whether to grant a data access request. Like in other cases, such DSC may lack knowledge or motivation to adequately consider the interests of at least some categories of users of the platform—especially SMEs.

Public databases on online advertising

A measure that raises similar concerns is the planned "online advertising transparency" of very large online platforms (Article 30). Such platforms will have a duty to create public repositories including detailed information on all advertisements like the targeting criteria used. According to some amendments proposed in the European Parliament, this information would also include the cost of the particular advertisement.

This measure constitutes a very grave, even existential, threat to many SMEs that reach their customers by advertising on very large online platforms. Competitors—especially large competitors—will be able to copy the advertising strategies of SMEs particularly successful in using online advertising. This way the competitive advantage of such SMEs may be destroyed in an

instant. Moreover, SMEs that specialize in advising on online marketing strategies will be similarly negatively affected as their know-how will largely become public.

No such general transparency exists for offline advertising. This measure would impose significant burdens on doing business online, which are absent offline. It may seem that the data on advertising on very large online platforms may be easier to report than that on physical billboards, television advertisements and so on. But this doesn't provide a sufficient reason to make the online advertising data public, while the offline advertising data is not.

It is thus hard to see how such a measure can be seen as proportionate outside of some specific contexts like political advertising, where the public interest in transparency may be stronger.

References

Civil Society Joint Statement. (2021). *Civil Society Joint Statement on the Draft Report on the Digital Services Act*. Center for Democracy & Technology. Available at: https://cdt.org/wp-content/uploads/2021/06/07-08-UPDATED-2021-06-30-CDT-Europe-Comments-to-IMCO-in-advance-of-deadline-for-tabling-AMs-1st-July.pdf

Eurostat. (2018). "Social media use by type, internet advertising". Available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_cismt/default/table?lang=en

Husovec, M. (2021). '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (September 17, 2021). *SSRN*. Available at: https://ssrn.com/abstract=3784149

Kaye, D. (2018). *Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. United Nations. Available at: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35

Keller, D. (2015). 'Empirical Evidence Of "Over-Removal" By Internet Companies Under Intermediary Liability Laws'. *Center for Internet and Society at Stanford Law School.* Available at: https://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws

Oxford Economics. (2020). *Digital Services in Europe: An Evidence Review*. Available at: https://www.oxfordeconomics.com/recent-releases/Digital-services-in-Europe