The EU Digital Services Act and academic research

David Clark

July 2023

A working paper of the CAIDA GMI3S project.[1]

1 Background

The EU Digital Services Act (DSA)[2] is intended to reduce the risks and challenges for individual recipients of Digital Information services, in particular what are described as intermediate services. The regulation imposes specific obligations on platforms that allow online trading, and expanded obligations on very large online platforms and very large search engines.

A second goal of the DSA is to provide a single, harmonized regulatory framework for the Union, and to preempt the creation of divergent regulatory structures by individual States. The regulation states that Member States should not adopt or maintain additional national requirements relating to the matters falling within the scope of this Regulation.[3]

The Act establishes an independent advisory group of Digital Services Coordinators on the supervision of providers of intermediary services named 'European Board for Digital Services' (the 'Board').[4]

The regulation is structured as a long preamble, with many sections discussing the motivation and intent of the Act, and the regulations themselves, structured as a number of Articles. In explaining the Act, I often quote from the preamble, which is a more expansive and contextual discussion of the regulations.

In this working paper I provide a summary of the objectives of the regulation, the nature of the harms they contemplate, and the types of specific regulatory obligations.

I also summarize the elements of the Act that are intended to ensure that independent, third-party researchers such as academics have access to the data necessary to understand the nature of the harms and the effectiveness of the mitigations. The Act creates rules that enable and encourage the academic community to work with proprietary data, sending an important signal that the EU intends to make their academic research establishment a recognized part of shaping the future of the Internet in the Union.

2 Scope of authority

The regulation applies to what are termed intermediate services. Such services include 'mere conduit', 'caching' and 'hosting' services.

> *'Mere conduit' intermediary services include generic categories of services, such as internet exchange points, wireless access points, virtual private networks, DNS services and resolvers, top-level domain name registries, registrars, certificate authorities that issue digital certificates, voice*

[1]This material is based on research sponsored by the National Science Foundation (NSF) grant OAC-2131987. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of NSF.

[2] [Eur22]

[3]ibid, pg 3, section 9

[4]ibid, pg 87, Article 67

over IP and other interpersonal communication services, while generic examples of 'caching' intermediary services include the sole provision of content delivery networks, reverse proxies or content adaptation proxies. [5]

The Act imposes a number of explicit obligations on what are called very large online platforms and very large search engines.

> *Very large online platforms and very large online search engines may cause societal risks, different in scope and impact from those caused by smaller platforms. Providers of such very large online platforms and of very large online search engines should therefore bear the highest standard of due diligence obligations, proportionate to their societal impact.*[6]

I summarize the obligations in Section 4.

As of 25 April, the Commission has made the following designations:

Very Large Online Platforms:

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

[5] ibid, pg 8, section29
[6] ibid, pg 21, section 76.

Very Large Online Search Engines:

- Bing
- Google Search

The Act applies to services that are made available to users in the Union, independent of where they are located.

> *In order to ensure the effectiveness of the rules laid down in this Regulation and a level playing field within the internal market, those rules should apply to providers of intermediary services irrespective of their place of establishment or their location, in so far as they offer services in the Union, as evidenced by a substantial connection to the Union.*[7]

3 Contemplated harms

The harms they contemplate relate to dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate. The overall objective is to ensure a safe, predictable and trusted online environment, within which fundamental rights enshrined in the Charter are effectively protected and innovation is facilitated.

Illegal content

> *"The concept of 'illegal content' should broadly reflect the existing rules in the offline environment. In particular, the concept of 'illegal content' should be defined broadly to cover information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities. Illustrative examples include the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer protection law, the non-authorised use of copyright protected material, the illegal offer of accommodation services or the illegal sale of live animals."* [8]

Manipulative system design Another class of harm is system design that leads to manipulation of users.

> *Dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them. Providers of online platforms should therefore be prohibited from deceiving or nudging recipients of the service and from distorting or impairing the autonomy, decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof.*[9]

Advertising Advertising is considered a significant source of risk.

[7] ibid, pg 2, section 7
[8] ibid, pg 5, section 12
[9] ibid, page 18, section 67

Online advertising can contribute to significant risks, ranging from advertisements that are themselves illegal content, to contributing to financial incentives for the publication or amplification of illegal or otherwise harmful content and activities online, or the discriminatory presentation of advertisements with an impact on the equal treatment and opportunities of citizens. In addition to the requirements resulting from Article 6 of Directive 2000/31/EC, providers of online platforms should therefore be required to ensure that the recipients of the service have certain individualised information necessary for them to understand when and on whose behalf the advertisement is presented. They should ensure that the information is salient, including through standardised visual or audio marks, clearly identifiable and unambiguous for the average recipient of the service, and should be adapted to the nature of the individual service's online interface. In addition, recipients of the service should have information directly accessible from the online interface where the advertisement is presented, on the main parameters used for determining that a specific advertisement is presented to them, providing meaningful explanations of the logic used to that end, including when this is based on profiling.[10]

When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities, this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups. Online platforms are particularly sensitive environments for such practices and they present a higher societal risk.[11]

Systemic risks The Act refers to a class of harm called *systemic risks*.

Very large online platforms and very large online search engines can be used in a way that strongly influences safety online, the shaping of public opinion and discourse, as well as online trade. The way they design their services is generally optimised to benefit their often advertising-driven business models and can cause societal concerns. Effective regulation and enforcement is necessary in order to effectively identify and mitigate the risks and the societal and economic harm that may arise. Under this Regulation, providers of very large online platforms and of very large online search engines should therefore assess the systemic risks stemming from the design, functioning and use of their services, as well as from potential misuses by the recipients of the service, and should take appropriate mitigating measures in observance of fundamental rights.[12]

The Act discusses four classes of systemic risks[13]:

- "[R]isks associated with the dissemination of illegal content, such as the dissemination of child sexual abuse material or illegal hate speech or other types of misuse of their services for criminal offences, and the conduct of illegal activities, such as the sale of products or services prohibited by Union or national law, including dangerous or counterfeit products, or illegally-traded animals."
- "[T]he actual or foreseeable impact of the service on the exercise of fundamental rights, as protected by the Charter, including but not limited to human dignity, freedom of expression and of information, including media freedom and pluralism, the right to private life, data protection, the right to non-discrimination, the rights of the child and consumer protection. Such risks may arise, for example, in relation to the design of the algorithmic systems used by the very large online platform or by the very large online search engine or the misuse of their service through the submission of abusive notices or other methods for silencing speech or hampering competition.

[10] ibid, page 19, section 68
[11] ibid, pg 19, section 69
[12] ibid, pg 22, section 79
[13] ibid, pp 22-23, sections 80-83)

- "[T]he actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, as well as public security."
- "[T]he design, functioning or use, including through manipulation, of very large online platforms and of very large online search engines with an actual or foreseeable negative effect on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence. Such risks may also stem from coordinated disinformation campaigns related to public health, or from online interface design that may stimulate behavioural addictions of recipients of the service."

These sections from the preamble elaborate on the concept of systemic risk.

> *When assessing such systemic risks, providers of very large online platforms and of very large online search engines should focus on the systems or other elements that may contribute to the risks, including all the algorithmic systems that may be relevant, in particular their recommender systems and advertising systems, paying attention to the related data collection and use practices. They should also assess whether their terms and conditions and the enforcement thereof are appropriate, as well as their content moderation processes, technical tools and allocated resources. When assessing the systemic risks identified in this Regulation, those providers should also focus on the information which is not illegal, but contributes to the systemic risks identified in this Regulation. Such providers should therefore pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation. Where the algorithmic amplification of information contributes to the systemic risks, those providers should duly reflect this in their risk assessments. ... Providers of very large online platforms and of very large online search engines should, in particular, assess how the design and functioning of their service, as well as the intentional and, oftentimes, coordinated manipulation and use of their services, or the systemic infringement of their terms of service, contribute to such risks. Such risks may arise, for example, through the inauthentic use of the service, such as the creation of fake accounts, the use of bots or deceptive use of a service, and other automated or partially automated behaviours, which may lead to the rapid and widespread dissemination to the public of information that is illegal content or incompatible with an online platform's or online search engine's terms and conditions and that contributes to disinformation campaigns.*[14]
>
> *Providers of very large online platforms and of very large online search engines should also be diligent in the measures they take to test and, where necessary, adapt their algorithmic systems, not least their recommender systems. They may need to mitigate the negative effects of personalised recommendations and correct the criteria used in their recommendations. The advertising systems used by providers of very large online platforms and of very large online search engines can also be a catalyser for the systemic risks.*[15]

The concept of *systemic risks* is important because it scopes the problems for which the Act provides a specific right of access to data for third-party researchers.

4 Rights and obligations specified by the DSA

The regulation establishes:
(a) a framework for the conditional exemption from liability of providers of intermediary services;
(b) rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services;
(c) rules on the implementation and enforcement of this Regulation, including as regards the cooperation of and coordination between the competent authorities.

[14] ibid. pg 23, section 84
[15] ibid, pg 24, section 88

4.1 Protection from liability

- Providers of mere conduit are protected from liability for the content they transmit, so long as they do not initiate the transmission, select the receiver, or modify the content.
- Providers of caching services are protected from liability for the content they cache so long as they do not modify the content, comply with conditions for access, comply with rules reguarding the updating of the information, do not interfere with the use of tools used by industry to track the use of the information, and quickly remove cached copies of information if they become aware that the original copy has been removed.
- Providers of hosting services are protected from liability for the content they store on behalf of a user of the service so long as they have no actual knowledge of illegal activity or illegal content, and so long as they act expiditiously to remove or block access to such content upon obtaining such knowledge.

They can act voluntarily to deal with illegal content without losing this protection, and have no general obligation to monitor.

4.2 Obligations applying to all covered entities

- Provide a single point of contact for regulators and for recipients of their service.
- Identify a legal representative if they do not have an establishment in the Union.
- Provide clear terms and conditions.
- Provide a transparency report with the number of orders and notices related to illegal content, information about voluntary content moderation, number of complaints about removal of content, and uses of automated means for content moderation.

4.3 Additional obligations on hosting services

- Provide a mechanism to report illegal content.
- Provide a clear reason to affected parties for any action to remove content.
- Promptly inform law enforcement agencies if they become aware of information leading to suspicion of a criminal offense involving threat to life or safety of persons.

4.4 Additional obligations on online platforms

With the exception of micro and small enterprises:

- Implement an internal complaint-handling system.
- Allow out of court dispute resolution.
- Suspend users who frequently provide manifestly illegal content.
- Facilitate the processing of notices submitted by *trusted flaggers*.
- As part of transparency reporting, list number of disputes referred to out of court resolution and number of suspensions.
- Shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.

- For each advertisement, provide a means accessible from the advertisement for the recipient to determine that the information is an advertisement, the natural or legal person on whose behalf the advertisement is presented and who paid for it, and the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters.
- Provide to the users of the platform information on the main parameters used in their recommender systems, including the criteria that are most important in determing what is recommended, and the reasons for the importance of these criteria.
- Protect the safety, privacy and security of minors.

4.5 Additional obligations of platforms that support trading

With the exception of small and micro traders:

- Obtain the name, address, telephone number and email address of traders, as well as any required identification documentation.
- Design their systems so that by design traders can comply with required regulatory obligations.
- Given actual knowledge, inform purchasers of any illegal products.

4.6 Additional obligations of very large platforms and search engines

- Diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.
- Put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified
- During a crisis, assess whether their service contributes to a significant threat, and apply specific, effective and proportionate measures to mitigate these threats.
- Engage annual independent third-party auditing of compliance.
- Provide at least one option for a recommender system that is not based on profiling (as defined).
- Compile and make publicly available a searchable and reliable repository containing the specified information concerning ad placement.
- Provide access for the regulator to data necessary to verify compliance.
- Establish a compliance function, which is independent from their operational functions.
- Pay an annual supervisory fee to the Commission.
- Develop voluntary standards and codes of conduct, including codes for online advertising and accessibility. The Commission will encourage and facilitate these actions.

5 Data access to indepdent researchers

The Act includes specific requirements on providers of very large services to make available, on demand from the regulatory bodies, access to data requested by independent "vetted researchers". This obligation is specified in Article 40 of the Act, as follows:

Article 40
Data access and scrutiny

1. Providers of very large online platforms or of very large online search engines shall provide the Digital Services Coordinator of establishment or the Commission, at their reasoned request and within a reasonable period specified in that request, access to data that are necessary to monitor and assess compliance with this Regulation.

2. Digital Services Coordinators and the Commission shall use the data accessed pursuant to paragraph 1 only for the purpose of monitoring and assessing compliance with this Regulation and shall take due account of the rights and interests of the providers of very large online platforms or of very large online search engines and the recipients of the service concerned, including the protection of personal data, the protection of confidential information, in particular trade secrets, and maintaining the security of their service.

3. For the purposes of paragraph 1, providers of very large online platforms or of very large online search engines shall, at the request of either the Digital Service Coordinator of establishment or of the Commission, explain the design, the logic, the functioning and the testing of their algorithmic systems, including their recommender systems.

4. Upon a reasoned request from the Digital Services Coordinator of establishment, providers of very large online platforms or of very large online search engines shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraph 8 of this Article, for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union, as set out pursuant to Article 34(1), and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35.

5. Within 15 days following receipt of a request as referred to in paragraph 4, providers of very large online platforms or of very large online search engines may request the Digital Services Coordinator of establishment, to amend the request, where they consider that they are unable to give access to the data requested because one of following two reasons:
(a) they do not have access to the data;
(b) giving access to the data will lead to significant vulnerabilities in the security of their service or the protection of confidential information, in particular trade secrets.

6. Requests for amendment pursuant to paragraph 5 shall contain proposals for one or more alternative means through which access may be provided to the requested data or other data which are appropriate and sufficient for the purpose of the request.

The Digital Services Coordinator of establishment shall decide on the request for amendment within 15 days and communicate to the provider of the very large online platform or of the very large online search engine its decision and, where relevant, the amended request and the new period to comply with the request.

7. Providers of very large online platforms or of very large online search engines shall facilitate and provide access to data pursuant to paragraphs 1 and 4 through appropriate interfaces specified in the request, including online databases or application programming interfaces.

8. Upon a duly substantiated application from researchers, the Digital Services Coordinator of establishment shall grant such researchers the status of 'vetted researchers' for the specific research referred to in the application and issue a reasoned request for data access to a provider of

very large online platform or of very large online search engine a pursuant to paragraph 4, where the researchers demonstrate that they meet all of the following conditions:
(a) they are affiliated to a research organisation as defined in Article 2, point (1), of Directive (EU) 2019/790;
(b) they are independent from commercial interests;
(c) their application discloses the funding of the research;
(d) they are capable of fulfilling the specific data security and confidentiality requirements corresponding to each request and to protect personal data, and they describe in their request the appropriate technical and organisational measures that they have put in place to this end;
(e) their application demonstrates that their access to the data and the time frames requested are necessary for, and proportionate to, the purposes of their research, and that the expected results of that research will contribute to the purposes laid down in paragraph 4;
(f) the planned research activities will be carried out for the purposes laid down in paragraph 4;
(g) they have committed themselves to making their research results publicly available free of charge, within a reasonable period after the completion of the research, subject to the rights and interests of the recipients of the service concerned, in accordance with Regulation (EU) 2016/679.
Upon receipt of the application pursuant to this paragraph, the Digital Services Coordinator of establishment shall inform the Commission and the Board.

9. Researchers may also submit their application to the Digital Services Coordinator of the Member State of the research organisation to which they are affiliated. Upon receipt of the application pursuant to this paragraph the Digital Services Coordinator shall conduct an initial assessment as to whether the respective researchers meet all of the conditions set out in paragraph 8. The respective Digital Services Coordinator shall subsequently send the application, together with the supporting documents submitted by the respective researchers and the initial assessment, to the Digital Services Coordinator of establishment. The Digital Services Coordinator of establishment shall take a decision whether to award a researcher the status of 'vetted researcher' without undue delay.

While taking due account of the initial assessment provided, the final decision to award a researcher the status of 'vetted researcher' lies within the competence of Digital Services Coordinator of establishment, pursuant to paragraph 8.

10. The Digital Services Coordinator that awarded the status of vetted researcher and issued the reasoned request for data access to the providers of very large online platforms or of very large online search engines in favour of a vetted researcher shall issue a decision terminating the access if it determines, following an investigation either on its own initiative or on the basis of information received from third parties, that the vetted researcher no longer meets the conditions set out in paragraph 8, and shall inform the provider of the very large online platform or of the very large online search engine concerned of the decision. Before terminating the access, the Digital Services Coordinator shall allow the vetted researcher to react to the findings of its investigation and to its intention to terminate the access.

11. Digital Services Coordinators of establishment shall communicate to the Board the names and contact information of the natural persons or entities to which they have awarded the status of 'vetted researcher' in accordance with paragraph 8, as well as the purpose of the research in respect of which the application was made or, where they have terminated the access to the data in accordance with paragraph 10, communicate that information to the Board.

12. Providers of very large online platforms or of very large online search engines shall give access without undue delay to data, including, where technically possible, to real-time data, provided that the data is publicly accessible in their online interface by researchers, including those affiliated to not for profit bodies, organisations and associations, who comply with the conditions set out in paragraph 8, points (b), (c), (d) and (e), and who use the data solely for performing research that contributes to the detection, identification and understanding of

systemic risks in the Union pursuant to Article 34(1).

13. The Commission shall, after consulting the Board, adopt delegated acts supplementing this Regulation by laying down the technical conditions under which providers of very large online platforms or of very large online search engines are to share data pursuant to paragraphs 1 and 4 and the purposes for which the data may be used. Those delegated acts shall lay down the specific conditions under which such sharing of data with researchers can take place in compliance with Regulation (EU) 2016/679, as well as relevant objective indicators, procedures and, where necessary, independent advisory mechanisms in support of sharing of data, taking into account the rights and interests of the providers of very large online platforms or of very large online search engines and the recipients of the service concerned, including the protection of confidential information, in particular trade secrets, and maintaining the security of their service.

An important limitation on this Article is that the scope of research to which it applies is the study of *systemic risk*. I discuss the concept of systemic risk in Section 3.

References

[Eur22] European Commission. Regulation (eu) 2022/2065 of the european parliament and of the council of 19 october 2022 on a single market for digital services and amending directive 2000/31/ec (digital services act), 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014.