CEP POLICY PAPER

EU Commission consultation Digital Services Act package – ex ante regulatory instrument of very large online platforms acting as gatekeepers

May 2021

Alexander Ritzmann, Dr. Hans-Jakob Schindler and Lucinda Creighton

Executive Summary

- The business model of most very large social media and video sharing platforms (gatekeepers), which is based on extracting and monetizing as much data from their users by manipulating them to spend as much time as possible on their platforms, might currently be creating societies that are "… addicted, outraged, polarized, performative and misinformed".[1] The harmful effects for users and societies at large are systemic and by design and cannot be characterized as unintended consequences of an otherwise healthy and well-functioning business model.[2] Margrethe Vestager, Executive Vice President of the European Commission for A Europe Fit for the Digital Age, has called very large tech companies "threats to democracy and anticompetitive".[3]

- The draft Digital Services Act (DSA) is a welcomed and ambitious piece of legislation that aims "to create a safer digital space in which the fundamental rights of all users of digital services are protected".[4] Unfortunately, despite introducing some promising new elements like increased transparency requirements and external audits, in its current form the draft will most likely fall short of its main objective.

- The draft DSA is based on a set of narratives about the role, function and business models of so-called gatekeeper platforms that do not seem to adequately reflect their actual functionality and commercial purpose. This paper will therefore address those systemic misunderstandings and provide an alternative narrative that might help to build the internet and intermediary services the EU is actually aiming for.

- The principle of the proposed limited liability regime of the DSA of 2020 is mostly based on a 62-year-old US court decision which stated that a newsstand owner, who was arrested in 1956 for selling a book with "indecent" content, cannot be held liable for the content of books he was selling, unless he knew (or should have known) about their illegal content.[5] This special privilege serves multi-billion dollar tech companies until today and is currently being challenged in the United States, but not in the DSA draft.

- It is particularly relevant to highlight that the limited liability regime of the existing EU e-Commerce directive and the current draft of the DSA actually allows for a proactive moderation of user-generated content by the companies. This is sometimes called the Good Samaritan clause. It maintains the limits of their liability for the remaining illegal content on their platform if they proactively moderate content on a voluntary basis. However, the limited liability regimes in the EU regulations did not, and still do not, provide any positive or negative incentives for the companies to invest in effective proactive content moderation.

- From a purely business perspective, it is reasonable for a for-profit company to ask why they should allocate elite and expensive data engineers to build effective content moderation systems, if the same engineers instead could grow the revenue side of the business model. Also, it appears to be much less expensive for the companies to hire more and more public policy managers who "handle" upset and concerned policy makers and civil society organizations criticizing the individual and societal harm created by the constant and massive availability of illegal and harmful content on their services.

- The argument that limited liability created a fertile ground for innovation might or might not have been correct in the past, considering all the benefits and harms that have been created by the gatekeepers. It is obvious, however, that for the past several years, innovation for gatekeepers mostly means buying innovative smaller companies and thereby consolidating or growing their market dominance. The fact that a limited liability regime for tech startups from 1996 is still supposed to be applied to market dominating gatekeeper companies in 2021 and beyond should be seen as a policy failure of the European Union and its Member States.

- If EU policymakers and EU citizens want very large for-profit private companies to host and facilitate safe public spaces for freedom of opinion and democracy, then draft legislation needs to mandate or incentivize companies to do so and potentially also pay them for this new service, which is most likely not compatible with their existing business model.

- While it is beyond the scope of this paper to develop a less toxic business model for social media and video sharing platforms, the current limited liability regime most likely would need to be terminated or significantly narrowed in scope, moving away from the "exceptionalism" approach currently employed towards the tech industry. Furthermore, an obligation for gatekeepers to proactively monitor their platforms for illegal content should be introduced. It remains unclear why today systemic proactive monitoring measures and upload filters can be applied in an untransparent manner for for-profit purposes of the companies but not in a transparent manner for the public interest of user protection from illegal and/or harmful content.

- Since the new audit and compliance regime that the DSA envisions for gatekeepers is a positive development and mirrors in significant aspects regimes already deployed in other industries, we urgently advise to include key learnings which were introduced after major failings and crisis particularly as it relates to failures of audit systems in the financial industry. These includes a) provisions that require platforms to allow auditors access to all relevant information during annual and additional audits b) ensuring commercial independence of auditors by creating an industry wide auditing fund from which auditors are going to be compensated, c) strengthening the independence of auditors by requiring the rotation of auditing mandates, and d) requiring separation of auditing and consulting mandates.

About CEP and the authors

The Counter Extremism Project (CEP) is an international, nonprofit policy organization that has been engaged in efforts to effectively regulate social media and video sharing companies[6] since 2015. Our focus lies on extremist ideologies and on illegal and terrorist content online. CEP advisors have been working with EU institutions and EU Member States for the past several years on some of the key issues the DSA aims to regulate.

Alexander Ritzmann is a Senior Advisor to CEP and to the European Commission's Radicalisation Awareness Network (RAN) as well as an Associate Fellow at the German Council of Foreign Relations (DGAP).

Dr. Hans-Jakob Schindler is Senior Director at CEP and head of its Berlin/Germany office. He is the former Coordinator of the ISIL, Al-Qaida and Taliban Monitoring Team of the United Nations Security Council.

Please direct inquiries regarding this paper to Marco Macori, CEP Research Fellow: mmacori@counterextremism.com / https://www.counterextremism.com/

Table of Content

Overall assessment of the DSA

In September 2020, CEP contributed to the first round of consultations[7], particularly asking for the DSA to:

- Stop algorithmic amplification of illegal content
- Mandate clear and understandable transparency
- Learn from the NetzDG: "notice and take down" is insufficient
- Require proactive search for illegal content
- Learn from the regulatory and compliance structures (and failures) of the financial industry and others

The DSA draft published by the commission in December 2020 is an ambitious piece of legislation that aims, amongst other objectives, “to create a safer digital space in which the fundamental rights of all users of digital services are protected”. [8]

Judging the draft legislation by this objective, CEP appreciates that stopping the algorithmic proliferation of illegal content and mandating understandable transparency (Art. 13, Art. 23, Art. 29 and Art. 33) are some of the core aspects the draft DSA aims at enforcing.

Unfortunately, the draft legislation does not address the continued failure of the existing “notice and action” moderation systems (Article 14) of gatekeepers.[9] These have been highlighted repeatedly in studies and tests both by CEP and other organizations such as jugendschutz.net.[10] On the contrary, the DSA perpetuates the “notice and action” mechanism as the main content moderation system, expecting the 400.000.000 internet users in the EU first to be exposed to illegal and possibly harmful content and then to notify the platforms about it. This means the externalization of safety and security functions to users rather than a requirement for platforms to ensure the safety of their customers or prevent harmful effects on the societies in which they conduct their commercial activities.

Article 19 pushes for gatekeepers to work with ‘trusted flaggers’ and other professional third parties, including governmental Internet Referral Units (IRUs), whose current mandate in most cases is limited to Islamist extremism/terrorism. While studies have shown that illegal content reported by trusted flaggers has a higher chance of being taken down or blocked than if the exact same illegal content is reported by users only, the DSA draft lacks clarity on how those trusted flaggers should be funded. At the moment, many trusted flagger organizations are civil society organizations that provide their expertise in the framework of small and short-term projects commissioned by governments. Those trusted flaggers mostly manually search for illegal content and are by no means capable of monitoring the billions of pieces of content that are produced by users each day on very large global platforms.

Lessons learned from CEP’s testing of gatekeepers “notice and action” systems

The draft also prohibits a general obligation (Article 7) to monitor information that intermediaries transmit or store and respectively does not mandate gatekeeper platforms to a proactive search for illegal content. As mentioned above, several evaluations and tests of the German NetzDG[11] “notice and action” mechanisms demonstrate that neither users nor trusted flaggers are capable of providing the effective moderation needed to ensure that gatekeeper platforms are significantly safer. If the proposed content moderation approach contained in the current draft of the DSA remains unchanged, it is mostly left up to the decision of for-profit tech companies on how they may or may not protect their users.

During the CEP tests of gatekeepers “notice and action” mechanisms, two major lessons emerged:[12]

Lesson 1: "notice and action" systems might not work properly

For example, YouTube only blocked or deleted 35% of the reported manifestly illegal extremist/terrorist videos, despite the fact that the notice given by CEP included information about the official government ban orders which had been also confirmed by court decisions. Videos with identical content were blocked in some cases but not others, which further indicates that the applied system or process is defective or at minimum significantly inconsistent in its decision making.

- After a months-long process following the publication of CEP findings, Google Germany confirmed that they agreed with CEPs classifications of the reported content, which was then blocked by YouTube according to the NetzDG.

Lesson 2: "notice and action" systems, even if they work properly, might not achieve the objectives set by the current DSA proposals

Facebook blocked manifestly illegal images reported by CEP but did not do so with unreported, manifestly illegal images in the same photo folder within the same Facebook account.

- Only after the publication of CEPs findings, Facebook removed the account in total. This indicates that “notice and takedown” is being implemented only in the narrowest possible manner and does not present an early warning system for the company, leading to more strategic defences against remaining manifestly illegal content, even when present within the same user account.

The DSA proposes new transparency requirements and external audits, which CEP very much welcomes in general. The lack of procedural clarity, however, might make those insufficient. Particularly, lessons from (failed) auditing/compliance systems for example from the financial sector, are largely ignored but should be at the centre of a DSA auditing framework.

Unfortunately, the DSA is still based on, and helps to continue spreading, a set of misinformed narratives about the status quo of the role, function and business models of so-called gatekeeper platforms. This paper will therefore first try to address those systemic misunderstandings and provide an alternative narrative that might help to build the internet and intermediary services the EU is actually aiming for. Secondly, we are sharing concrete learnings from the financial industry that should be implemented within the existing DSA draft.

Part A)

Towards a new understanding of "social" media and possible alternative business models that can actually protect EU citizens and serve European democracies

1) Systemic flaws and significant misunderstandings in the draft EU Digital Services Act

Humans need stories to make sense of the world. Over the course of the last decade, different narratives have been developed and shard that describe very large for-profit social media and video sharing companies as beacons of free speech that need special legal privileges to foster innovation and market competition. While it is possible that, particularly in the United States, those narratives may have been feasible 10 or 15 years ago, it appears abundantly clear that they no longer serve the interest of the 400.000.000 internet users in the European Union.

While it might feel like the platforms have been mandated to serve as safe public spaces for the free exchange of opinions, their contributions to the democratic discourses are voluntary and arbitrary, much more like social engagement activities of other for-profit companies like BMW or McDonald's, which actually have another core business model and purposes.

The "social" part of the social media industry is only the means to the end of creating income through the advertisement business by extracting, storing, analyzing, manipulating, processing and monetizing all available user data.

While some court decisions,[13] e.g. in Germany, find that particularly gatekeepers serve "de facto" as public squares and have to protect fundamental rights, they rather accidentally slipped into this role for which they were neither designed, prepared or are regulated for.

2) Building an outraged and misinformed society

The business model of social media, which aims at extracting and monetizing as much data from their users by manipulating them to spend as much time as possible on their platform, might actually be creating "…a society that is addicted, outraged, polarized, performative and misinformed".[14] Or as Harvard Professor Dr. Joan Donovan put it at a recent US Senate hearing: "Misinformation at scale is a feature of social media, not a bug".[15] Margrethe Vestager, Executive Vice President of the European Commission for A Europe Fit for the Digital Age, has called very large tech companies "threats to democracy and anticompetitive".[16]

Facebook provides a recent practical example[17] of a gatekeeper business model. If a user in Germany searches for mixed martial arts events or groups on the platform, a leading violent extreme right-wing organization called "Kampf der Nibelungen" (KdN) will be displayed at some point. If the user then selects for this group, a "we want to protect our community" disclaimer will appear explaining that KdN, which is highlighted in several German domestic intelligence reports[18] as a major violent extreme right-wing transnational actor[19], "could be extremist". Facebook then offers the user to either click on KdN, which will lead them to a vast network of extreme right-wing groups and propaganda/merchandise stores on Facebook, or to click on the "protect our community" button which will redirect them to a civil society organization that works on preventing and countering violent extremism (P/CVE). On that same page, where all this is happening, Facebook will also place a very large advertisement.

Summed up, Facebook helps users to not only find violent extremist content on their platform but will also provide the users with the opportunity to go down the tunnel of extreme right subculture and online shops. At the same time, Facebook offers users to move to a website of a P/CVE civil society organisation.

At the same time, Facebook's content recognition systems place an advertisement making sure that, whatever decision the user makes, Facebook will make a profit. To be fair, most other gatekeepers, who also host KdN or similar content, don´t even try to nudge users in a different direction by placing a warning or indication that the content may be harmful.

This concrete example demonstrates that the harmful effects for users and societies at large[20] are systemic and by design, and should not be understood as unintended consequences of an otherwise healthy and well-functioning business model. This is, however, not to say that the intentions of the tech companies are bad, but rather that in the competition of liberal democratic values and financial revenue, revenue seems to be the priority, as would be expected for a commercial operation geared towards profit maximation.

If EU policymakers and citizens want social media to host and facilitate safe public spaces for freedom of opinion and democracy, then legislation should be drafted to mandate or incentivise companies to do so and potentially also pay them for this service, since this new mandate would very likely not be compatible with their existing business model of excessively harvesting, manipulating and monetizing user data.

Unfortunately, the draft DSA draft still promotes the above-mentioned outdated narratives about "social media" and, while acknowledging some of their flaws, tries to force a well-meaning compliance regime on the gatekeepers of an industry that operates on unfit and broken principles.

3) The DSA's fundamental regulative principle is outdated and unfit for purpose

The limited liability regime suggested in the DSA is providing the core framework of incentives for the actions of gatekeepers, specifically regarding the moderation of user-generated content. It is important to highlight that Articles 3, 4 and 5 of the DSA are based on the EU e-Commerce directive from the year 2000 (Articles 12-15), which is essentially mirroring section 230 of the Communications Decency Act (CDA) of the United States from 1996.[21]

This underlying regulatory principle states that no intermediary (online service provider) can be held liable for (illegal) third-party content on their platform, unless they knew or should have known that the content was illegal and if they acted in a mere technical, automatic and passive capacity.

The "limited liability" principle is grounded in the culture and legal tradition of the United States. Particularly the First Amendment,[22] which protects "free speech" much stronger, is relevant in this context compared to e.g. Article 10 of the European Convention, which puts several limitations on freedom of opinion in the European Union. [23] EU Member States then have their own legal definitions regarding illegal content and, for example, hate speech.

3.1) Are gatekeepers really the newsstand owners of the 21st century?

The legal principle underpinning the limited liability regulation for multi-billion tech companies today goes back to a US Supreme Court ruling from 1959, stating that a newsstand owner, who was arrested in 1956 for selling a book with "indecent" content, cannot be held liable for

the content of books he was selling, unless he knew (or should have known) about their illegal content. [24]

As stated in the decision of the US Supreme Court:

"The bookseller's limitation in the amount of reading material with which he could familiarize himself, and his timidity in the face of his absolute criminal liability, thus would tend to restrict the public's access to forms of the printed work which the State could not constitutionally suppress directly". [25]

As a reminder, the business model of many gatekeeper platforms is to use content recognition systems that analyze, process, manipulate and monetize all user activity and data from login to logoff (and sometimes beyond) to build user-avatars. Access to those user-avatars is then being sold to advertisement customers, enabling them to target their advertisements to predefined sets of users very specifically. In this process, social media build a "virtual reality" that is based on preferences and interests of users, but also on recommended and therefore manipulated content by the platforms to keep users engaged as long as possible with the platform and therefore also with the respective advertisements. Simply put, what users see on their Facebook, YouTube or Twitter profiles is supposed to keep them engaged with the service as long as possible to provide as much data to the platforms as possible. It remains unclear how this can be reconciled with the current DSA draft, which aims at mandating gatekeepers "…to develop appropriate risk management tools to protect the integrity of their services against the use of manipulative techniques".[26]

In conclusion, while there were several other relevant court cases in the US on the matter of liability for intermediaries like public broadcasters and telephone companies, the principle of the proposed limited liability regime of the DSA of 2020 is mostly based on a 62-year-old US court decision following the arrest of a newsstand owner in Los Angeles in 1956.

3.2) Learnings from the recent past: exceptionalism, market failure and monopolies

In the 1990s, US legislators who passed the Communications Decency Act aimed to protect their new tech industry and start-ups from over-regulation and provided it with this exceptional "wunderkind-privilege" of letting them grow without holding them responsible for their (lack of) content moderation. At the time legislators argued that users could simply use another service if they are unhappy with the content moderation approach of a specific platform.

Today, the DSA particularly aims at regulating gatekeepers who already dominate or monopolize their respective markets, making it difficult, if not impossible, for concerned users to simply switch to a competitor, because in many cases, these do not exist.

- In this context, it is particularly relevant to highlight that the limited liability regime of the US CDA, the EU e-Commerce directive and the current draft of the DSA actually allows for a proactive moderation of user-generated content by the companies.[27] This is sometimes called the Good Samaritan clause. It maintains the limits of their liability for the remaining illegal content on their platform if they proactively moderate content on a voluntary basis. However, the limited liability regimes in the US and EU regulations did not, and still do not, provide any positive or negative incentives for the companies to invest in effective (and costly) proactive content moderation.

From a business perspective, it is reasonable for a for-profit company to ask why they should allocate elite and expensive data engineers to build effective content moderation systems, if the same engineers instead could grow the revenue side of the business model.

Also, it appears to be much less expensive for the companies to hire more and more public policy managers who "handle" upset and concerned policy makers and civil society organizations criticizing the regular individual and societal harm created by the constant and massive availability of illegal and harmful content.

4) Why the big tech-companies welcome the draft DSA

Not surprisingly, major big-tech lobby associations like DOT.Europe "welcome that the current draft of the DSA maintains the core principles of the e-Commerce Directive's limited liability regime and even elevates them in the proposed Regulation".[28] This industry lobby group also claim that "the e-Commerce Directive (has) provided legal certainty for the development of innovative services in the Internal Market and ensured the protection of fundamental rights in the online space".[29]

From the perspective of the members of the mentioned association, which are for example Airbnb, Amazon, Facebook, Google, Microsoft, Spotify and TikTok, such a statement is to be expected.

The argument that limited liability created a fertile ground for innovation might or might not have been correct in the past, considering all the benefits and harms that have been created by the gatekeepers. It is obvious, however, that for the past several years, innovation for gatekeepers mostly means buying innovative smaller companies and thereby consolidating or growing their market dominance. [30]

Similar to all other industries, tech companies use existing legal frameworks and only invest in consumer protection when legally required or if significant risks or financial returns are to be expected. Hence, the fact that a fundamental principle of the current draft DSA, the limited liability regime from 1996, is still supposed to be applied to market dominating companies in 2021 and possibly the following decades, should first of all be seen as a policy failure of the European Union and its Member States.

In the US, the policy debate about amending or cancelling the limited liability regime of section 230 of the CDA is ongoing and of high priority for the Biden Administration as well as several leading members of the US Senate and House of representatives. [31]

5) Can big tech companies actually be audited at all?

While the proposed transparency requirements, external audits and possible penalties in the draft DSA might have an effect on the decision making of gatekeepers, it remains unclear how those compliance procedures will be implemented and enforced.

For example, it is highly questionable that external auditors have the actual insights and capacity today to effectively audit the company's "black box" algorithms and their multiple server farms worldwide. The automated decision-making systems developed and applied by gatekeepers might only be fully understood by a very small group of the tech company´s data engineers. The failures by the best and largest auditing firms worldwide in the past, investigating much less complex industries[32] indicate how difficult it could be to audit clients who have a highly complex and proprietary set of technology at the core of their business.

Importantly, the findings of the external audits proposed by the DSA are a foundation for the possible penalties that can be imposed on the respective companies.

6) How to build a safe internet for EU citizens

Today, asking that multi-billion-dollar (tech) companies not only follow a strict compliance regime, but also "own" the risks and damages their services might inflict on citizens and societies seems quite controversial. Unless, of course, such companies have led societies into global crises. It took the financial crisis of 2008 for policymakers to re-regulate the financial sector that was left to grow and compete with "innovative" financial products. And only after decades of resistance and an emerging climate crisis at hand, the automobile industry is slowly changing its toxic business model of using fossil fuels as the main energy sources for their products.

As outlined above, if EU policymakers and EU citizens want for-profit private companies to host and facilitate safe public spaces for freedom of opinion and democracy, then legislation should be drafted to mandate or at least incentivize companies to do so and potentially also pay them for this service, since this policy objective would be very likely not compatible with their existing business model of excessively harvesting, manipulating and monetizing user data.

Taking this thought further, if EU citizens and EU policy makers really want different platform behaviours regarding the hosting and algorithmic promotion of illegal and/or harmful content, the liability regime and the "exceptionalism" approach imported from the US needs to be terminated and this industry should be treated like any other industry commercially active in the EU. This would eventually mean the end of the existing business models of excessively harvesting, manipulating and monetizing user data for gatekeepers as well as for other companies operating along the same business model.

While it is beyond the scope of this paper to develop an alternative and less toxic business model for social media and video sharing platforms, an alternative to the currently limited liability regime could include an obligation for gatekeepers to proactively monitor the content on their platform for illegal content. It is important to highlight that these companies already very effectively moderate content based on their own commercially defined priorities, to monetize user data, prevent copyright infringements or to enforce their own community standards to ban and suppress legal but unwanted content for example. It remains unclear why today proactive monitoring measures and upload filters can be applied for for-profit purposes of the companies but not for the public interest of user protection.

In addition, a "know your user" requirement for companies, as well as liability for users who upload illegal content, similar to the "EU copyright directive", should be considered.

Due to the complexity of effectively auditing the "black box" algorithms, a special framework for "whistle blowers" and former big tech industry employees should be considered to overcome non-disclosure agreements former big-tech employees have to sign. Also, rewards for whistleblowers from gatekeeper companies should be considered.[33] In addition, incentives for relevant government agencies and private sector auditors could be given to recruit such "formers" in order to increase their relevant capacities.

Part B)

Lessons from (failed) auditing/compliance systems and recommendations for effective audits

I. Recommendations

Although significant questions currently remain on how audit systems in the tech industry may be effective,[34] it is also clear that any provisions that may be included in the DSA will require external and independent checks and audits to ensure their implementation by the obligated companies and to provide grounds to penalize the failure to do so. Therefore, the outline of an audit regime within the current draft of the DSA is generally a welcome and positive development. The audit regime the current draft of the DSA envisions for very large platforms mirrors in significant aspects audit regimes already deployed in other industries, in particular the financial industry. Given that the audit regime is envisioned to play a key role in ensuring compliance with the provision of the DSA at very large platforms, the following improvements should urgently be considered:

a) Revision of the definition of very large platforms in Article 25 to include additional platforms in the audit regime.

b) Including provisions that require platforms to allow auditors access to all relevant information during annual and additional audits by moving the relevant provisions from the preamble to Article 28.

c) Strengthening of the position of the compliance officer in very large platforms by dropping the provision that this function can be fulfilled on a contractual basis and requiring this function to be a full staff position in Article 32.

d) Ensuring commercial independence of auditors by creating an industry-wide auditing fund from which auditors are going to be compensated.

e) Strengthening the independence of auditors by requiring the rotation of auditing mandates every several years to avoid an integration between auditors and clients through long term cooperation which risks limiting the auditor's flexibility to make negative findings.

f) Requiring separation of auditing and consulting mandates in order to avoid commercial incentives for positive audit results in an effort to protect consultancy mandates.

II. Envisioned auditing system

II.I. Structure and function of audit regime

The proposed text of the DSA currently envisions an auditing system fairly similar to auditing regimes employed in other industries. In its current version, audit regimes only apply to very large platforms.[35]

Article 28 outlines the central provisions of the functioning of the audit regime for such platforms:

a) The audits are done annually and are financed by the platforms themselves (Art. 28.1.).

b) The audits encompass all relevant obligations of the DSA (Chapter III) and any codes of conduct (Art. 35) that the respective platform joins (Art. 28.1.a and b.).

c) Auditors are required to be independent, have proven expertise and objectivity (Art. 28.2. a, b and c.).

d) Apart from identifying information of the platform and the auditor, the audit report must include information on which specific elements were audited, what methodologies were used, and what the main findings were (Art. 28.2. a. to d.).

e) The audit report must include an opinion on whether the respective platform conformed with its obligation and if it is not the case also include operational recommendations on specific measures to achieve compliance (Art. 28.2. e. and f.).

f) The platform should take these recommendations into account, take action and one month after the audit report submit adopt an audit implementation report, outlining what measures were taken and – in case recommendations were not followed – why this is the case and what alternative measures were taken (Art. 28.2.i.).

Furthermore, the current version of the DSA explains that each very large platform has to appoint a compliance officer that is – among other duties – responsible for organising the audit activities (Art. 32.3.b.). Interestingly, while the compliance officer is required to report directly to the top management of a platform (Art. 32.6.), as is the case for compliance officers in the financial industry, Art. 32 allows that such an individual can work as a contractor/consultant (Art. 32.2.).

At the European Union level, the European Board for Digital Services, consisting of high-level personnel of the Commission, the national Digital Services Coordinators (DSCs), as well as other relevant authorities (by invitation) (Art. 48.1.) is also tasked with supporting national authorities to analyze the results of audit reports (Art. 49.a.)

II.II. Consequences of serious negative findings in audit reports

In case audit reports point towards serious and continuous infringements of a platform's obligations under the DSA., an investigation against the platform can be opened. In this case:

a) Auditors are required to submit information to the national DSCs (Art. 41.1.a.).

b) In case the "enhanced supervision system" (Art. 50) for a platform is enacted,[36] the national DSC of the jurisdiction in which the platform is established can request additional audits, at the expense of the platform, to assess the effectiveness the platform is taking to end the infringement of its obligations. These audit reports are then sent to the DSC, the Commission and the Board for Digital Services (Art. 50. 3.).

c) The Commission also has specific rights related to audits. It can request information concerning infringements both from the auditors as well as the platforms (Art. 52.1.), take interviews and statements for natural and legal persons in the framework of an investigation into infringements (Art. 53)[37] and carry out on-site inspections with the support of auditors (Art. 54.) as well as appoint auditors to assist it in its monitoring of platforms under enhanced supervision (Art. 57).

d) The investigation and enhanced supervision systems are enforced by the imposition of fines (Art. 41.2.c.) and periodic penalty payments (Art. 41.2.d) by the national DSC. These fines and payments are defined by the individual EU Member States (Art. 42). The Commission can also impose fines in case of non-compliance (Art. 59.1.) to punish refusal by a platform of its requests and decisions (Art. 59.2.) or periodic penalty payments to further enforce its decisions and requests (Art. 60.1.)

e) In cases where an infringement may cause a threat to life or the safety of persons the national DSC can also ask the judiciary of its EU Member State to order the temporary restriction of access to the respective service (Art. 41.3.b.). These restrictions are renewable as well repeatable (Art. 41.3.b.b.)

III. Potential to strengthen auditing regime and increase independence of auditors

III.I. Opportunities for general improvements

The envisioned audit system parallels, in general, audit systems deployed in other industries. The fact that it will only apply to very large platforms according to the definition in Art. 25 is justified with their particular significant impact on society.[38] The threshold of 10% of the European Union population[39] could be lowered to include more platforms being required to be audited. Defining such a threshold mirrors a similar provision in the German Network Enforcement Act (NetzDG).[40]

Given the crucial role that auditors are envisioned to play in the general monitoring of the compliance of very large platforms with the obligations under the DSA, it is surprising that access of these auditors to all relevant information is not included in the current provisions of Article 28. While it must be assumed that it is in the general interest of a platform to provide its auditors with the necessary access, it cannot be guaranteed that this will always be the case. Therefore, it may be advisable to move the relevant provisions from the preamble of the proposed DSA text to Article 28 to ensure that it becomes a legal obligation.[41]

Finally, the provision that the compliance officer of a very large platform can also be based on a contract rather than on a staff position (Art. 32.2.) is unusual when it comes to large scale industry players. A contract-based relationship is generally weaker than a staff arrangement. Therefore, it may not give the compliance officer the necessary standing in the internal hierarchy of a very large platform to effectively fulfil this function. Therefore, it may be advisable to drop this provision and require that the Compliance Officer to be a fully employed staff member of the respective platform.

III.II. Potential improvements based on experience in other industries

The financial crisis of 2008 and the collapse of several large corporations in the past 20 years have demonstrated three basic structural flaws in existing audit systems that limit the independence of auditors and therefore weaken the early warning function of such control systems. These are the direct commercial relationship between the control mechanism and the client, the creation of a client relationship that is too close to allow critical assessments of the client's performance and the combination of auditing and consulting mandates. These basic flaws should be avoided when setting up a new audit regime under the DSA.

III.II.I. Strengthening auditor independence through separating payment

The current DSA text outlines that all costs for regular and specific audits fall to the respective platform, while at the same time, the auditors are required to be independent of the platform. This is also the case in audit systems in other industries. However, it may be advisable to consider the economic power balance between an auditor and a very large platform if the platform directly compensates the auditor for its services.

As demonstrated during the 2008 financial crisis, investment banks directly compensated credit rating agencies for ratings of their mortgage-backed securities (MBS) and collateralized debt obligations (CDOs). This is seen as one of the significant causes of the financial crisis in 2008. Such direct payments provided financial incentives for the credit rating agencies to give more positive ratings for the respective MBS and CDOs as a positive rating would ensure that investment banks could sell the packages at higher prices on the market. Therefore, through positive ratings rating agencies ensured repeat business with investment banks.[42]

A similar financial incentive to issue positive audit reports may be created if very large platforms compensate their auditors directly. This is particularly the case as the annual audits of very large platforms will very likely be undertakings of significant size and therefore generate significant commercial interest and income for an auditor.

Therefore, it could be explored whether it may not strengthen the independence of an auditor if rather than direct payments, an industry-wide audit fund is created into which all platforms pay an annual membership fee based on their size. This fund would then reimburse the auditors, preventing a direct commercial relationship between a very large platform and an auditor.

III.II.II. Strengthening auditor independence through rotating audit mandates

The current version of Article 28 does not include a limit on how often a particular auditor can perform annual audits or provisions separating the functions of annual audits from those of the additional audits that the national DSCs or the Commission can require in the course of an investigation or the enhanced supervision system.

As the ENRON collapse in 2001 demonstrated, one aspect that prevented early detection of the highly unethical accounting practices and manipulation of its balance sheets through the misrepresentation of its earnings was its very close and long-standing relationship with the accounting firm Arthur Andersen LLP created through years of audits performed for ENRON exclusively by Arthur Andersen LLP.[43]

Therefore, it could be contemplated to ensure that annual audit mandates should be switched between auditors and that other business divisions of the auditors that conduct the annual audits cannot at the same time be employed as additional auditors during investigations and the enhanced supervision system. Given that annual audits of a very large platform will very likely be complex and require the building of specific capacities and expertise,[44] it seems advisable that this switching of auditors should only be required after several annual audits. For example, following the discovery of similar problems during the WIRECARD collapse in Germany, the German government is currently contemplating requiring rotating auditors once every 10 years.[45]

III.II.III. Strengthening auditor independence through separating audit from consulting mandates

One of the well understood weaknesses of existing audit systems relating to large corporations, which limits auditors' independence, is the combination of auditing and consulting services, offered by the same company to the same client.[46] Consultancy mandates can be commercially far more lucrative than audit mandates. Therefore, providing both functions to the same client may lead to a commercial incentive to provide the client with positive audit reports in order to ensure retention of existing and the procurement of new consultancy mandates. In order to counter this risk, the United Kingdom changed its regulations requiring the separation of audit and consultancy functions within large audit companies to limit such incentives.[47] An even stronger separation between auditing and consulting services, limiting the amount of consulting mandates an auditing company can perform for a client, is currently contemplated in Germany following the collapse of WIRECARD.[48]

Consequently, it may be advisable to include a provision in Article 28 of the DSA that ensures that such a separation of auditing and consulting mandates for the same client is required. Including such a provision in combination with the rotation of auditing mandates (see above

III.II.II.), would ensure that the commercial attractiveness of auditing mandates would be maintained as consulting services could be offered to all other very large platforms. Consulting services could again be offered to a respective platform when the auditing mandate is rotated.

---

[1] https://www.judiciary.senate.gov/meetings/algorithms-and-amplification-how-social-media-platforms-design-choices-shape-our-discourse-and-our-minds / (01:07)
[2] See for example: https://farid.berkeley.edu/downloads/publications/arxiv20.pdf or https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/ or https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html
[3] https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html
[4] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[5] Smith v. California, 361 U.S. 147 (1959), in: Kosseff, Jeff. The Twenty-Six Words That Created the Internet (P.35). Cornell University Press. 2019.
[6] When referring to companies, we mean the businesses who own the so-called social media or video sharing platforms which classify as gatekeepers according to the DSA definition, meaning they have at least 10% of all EU internet users as users on their services (also called very large platforms).
[7]https://www.counterextremism.com/sites/default/files/CEP%20Policy%20Paper_EU%20DSA_Sept%202020.pdf
[8] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN
[9] DSA definition: meaning they have at least 10% of all EU internet users as users on their platform(s).
[10] See for example: https://www.carlgrossmann.com/liesching-das-netzdg-in-der-praktischen-anwendung/
https://www.jugendschutz.net/fileadmin/download/pdf/Bericht_2019_2020_Islamismus_im_Netz.pdf
https://www.counterextremism.com/sites/default/files/CEP%20NetzDG%202.0%20Policy%20Paper%20April%202020%20ENG.pdf
[11] https://www.counterextremism.com/sites/default/files/Fighting-Hate-Speech-and-Terrorist-Propaganda-on-Social-Media-in-Germany.pdf
https://www.counterextremism.com/sites/default/files/CEP-CEPS_Germany%27s%20NetzDG_020119.pdf
[12]https://www.counterextremism.com/sites/default/files/CEP%20NetzDG%202.0%20Policy%20Paper%20April%202020%20ENG.pdf
[13] See for example: https://www.rv.hessenrecht.hessen.de/bshe/document/LARE190005741
[14] https://www.judiciary.senate.gov/meetings/algorithms-and-amplification-how-social-media-platforms-design-choices-shape-our-discourse-and-our-minds / (01:07)
https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/
[15] https://www.judiciary.senate.gov/meetings/algorithms-and-amplification-how-social-media-platforms-design-choices-shape-our-discourse-and-our-minds (0:55:20)
https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/
[16] https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html
[17] bit.ly/3srt70i (8:35)
[18] See for example: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2020/vsb-2019-en.html
[19] See for example:
https://www.counterextremism.com/sites/default/files/CEP%20Study_Violent%20Right-Wing%20Extremism%20and%20Terrorism_Nov%202020.pdf
[20] See for example: https://farid.berkeley.edu/downloads/publications/arxiv20.pdf
[21] See for example: https://harvardlawreview.org/2018/05/section-230-as-first-amendment-rule/
[22] See for example: Kosseff, Jeff. The Twenty-Six Words That Created the Internet (P.184). Cornell University Press. 2019 or: https://harvardlawreview.org/2018/05/section-230-as-first-amendment-rule/
[23] See for example: https://rm.coe.int/16806f5bb3 (P.7)
[24] Smith v. California, 361 U.S. 147 (1959).
[25] Kosseff, Jeff. The Twenty-Six Words That Created the Internet (P.35). Cornell University Press. 2019.
[26] DSA - CONTEXT OF THE PROPOSAL,

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN
[27] See for example: https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996
[28] https://doteurope.eu/wp-content/uploads/2021/04/DOT-Europe-DSA-Questions-and-Recommendations-Chapters-1-3-.pdf /
[29] https://www.bitkom.org/sites/default/files/2021-03/20210326_bitkom_position_dsa.pdf
[30] See for example: https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html
[31] See for example: https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html
[32] For example, the Enron case, the financial crisis in 2008, the Volkswagen "Dieselgate" or the Wirecard scandal (German online bank).
[33] For example: https://whistleblowersblog.org/2020/08/articles/global-whistleblowers/the-eu-campaign-for-whistleblower-rewards-a-new-idea-for-old-europe/ or https://voxeu.org/article/effective-rewards-whistleblowing
[34] See above: part A 5).
[35] Article 25 in its current form defines „very large platforms" as having an "average monthly active recipients of the service in the Union equal or higher than 45 million", See Article 25.1., https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en (referred to below as DSA-Proposal).
[36] This is the case if the DSC of the jurisdiction in which the respective platform is established (Art. 50.1.) finds that the platform has violated its obligations under Section 4 of Chapter III of the DSA (risk assessments, risk mitigation, audits, general transparency provisions, specific transparency of recommender system, data access to vetted researchers). The Commission, the European Board for Digital Services or a group of at least three national DSCs can also request.
[37] However, crucially only if these persons agree to be interviewed, meaning the Commission cannot require interviews or statements, only the provision of information is a requirement and penalties can be levied if incorrect or misleading information is provided (Art. 52.2. and Art. 59.2.a.).
[38] DSA-Proposal, page 3
[39] DSA-Proposal, page 3
[40] Paragraph 1 NetzDG defines the threshold for Germany as 2 million users, see: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html
[41] See paragraph 60 of the preamble.
[42] See for example: https://eu.usatoday.com/story/money/business/2013/09/13/credit-rating-agencies-2008-financial-crisis-lehman/2759025/
https://www.cfr.org/backgrounder/credit-rating-controversy
[43] See for example: https://www.nytimes.com/2002/01/15/business/enron-s-collapse-the-auditors-who-s-keeping-the-accountants-accountable.html
https://mpra.ub.uni-muenchen.de/1147/1/MPRA_paper_1147.pdf
[44] For which minimum industry standards for auditors should be agreed, including appropriate technical expertise, see above part A 5).
[45] https://www.ft.com/content/2f5c9ce0-76f5-47cb-9835-fcc2524062b6
https://www.wsj.com/articles/after-wirecard-germanys-proposed-audit-overhaul-worries-finance-executives-11617868813
[46] See for example: https://projekte.sueddeutsche.de/artikel/politik/deloitte-kmpg-pwc-ey-die-big-four-e945619/
https://www.ft.com/content/29a029a0-a7b2-11e8-8ecf-a7ae1beff35b
[47] See for example: https://www.washingtonpost.com/business/how-uk-audit-scandals-pushed-big-four-toward-split/2020/07/17/27eeb202-c817-11ea-a825-8722004e4150_story.html
[48] https://www.finance-magazin.de/banking-berater/wirtschaftspruefer/wirecard-was-bringt-eine-trennung-von-pruefung-und-beratung-2076281/
https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2020-10-26-Finanzmarktintegritaetsstaerkungsgesetz/1-Referentenentwurf.pdf?__blob=publicationFile&v=3