The next step towards auditing intermediaries

Ben Wagner 2022-02-23T12:30:48

The lack of transparency of digital platforms is a well-known problem that has wide societal implications. It has a detrimental impact on the exercise of rights of users, their ability to navigate in the online space and, ultimately, their ability to understand the world around them. Even more importantly, it fundamentally constraints any meaningful inquiry into how digital services influence our societies and thus makes introducing evidence-based and effective measures in the digital environment very difficult. Under the current state of affairs, the regulatory interventions in the digital environment are simply bound to be based on informed guesses, extrapolations from partial research findings or limited voluntary disclosures of the Big Tech companies. As a result, regulators can't effectively regulate and every effort to do so will keep missing its mark.

There is now an extraordinary opportunity to establish legally mandated criteria for meaningful transparency for online platforms in the proposed EU Digital Services Act (DSA). The proposal has just entered the final state of trilogue negotiations. It seeks to create safe digital spaces in compliance with fundamental rights. Perhaps the most novel element of the DSA is the set of due diligence safeguards, such as independent auditing of Very Large Online Platforms (VLOPs). However, the success of this mechanism will depend on the strength of oversight mechanisms which need to be accompanied by sufficient access to data. Hence, we propose creating an auditing intermediary to assure the effectiveness of such oversight. We argue that existing DSA proposals for independent audits will only be successful if they are independent *public* audits.

We don't really know anything about online platforms

Until very recently, efforts to address the profound lack of transparency and to enable data access currently guarded by online gatekeepers were rather scarce. True, some of the more recent pieces of legislation, either already in force (NetzDG) or in the making (DSA), are heading in the right direction. However, while containing measures legally mandating transparency reporting or data access frameworks, they still do not fully recognize the fact that a meaningful understanding of the digital environment requires an auditing process, where the data that is made available is not mediated by the platforms under scrutiny. An auditing framework could enable the independent verification of data that could then be made accessible to regulators and other key actors like civil society, journalists, or academia.

Meaningful transparency is an absolute prerequisite to efficient and legally sound regulation in the digital environment. But meaningful transparency is difficult to achieve, as any viable solution needs to navigate a perilous path. It needs to consider the sensitive nature of personal data, the risks of potential abuse of access to virtually unlimited data produced in the digital environment, the legal limits of the scope of inquiries within the competence of regulatory authorities and the commercial interests of regulated entities.

Our proposal: a public auditing intermediary

In our opinion, the best way to achieve meaningful transparency is by creating a public auditing authority that is equipped to provide all necessary safeguards to data access and deliver the needed insights efficiently. Given the ways in which VLOPs arbitrarily remove access to their platforms from academics and NGOs who wish to create transparency under the legal threats, as well as providing incorrect data to researchers in the context of the Social Science One initiative, the current status-quo is no longer acceptable. As recently leaked documents suggest, Facebook also regularly manipulates the design of systems to influence the quality of its transparency metrics, as well as the way in which those metrics themselves, anything short of rigorously auditing platform data cannot be trusted.

The DSA proposal on independent auditing of VLOPs under Article 28 looks encouraging at first. The proposal obliges VLOPs to undergo mandatory auditing performed by independent auditors. According to the Commission's technical briefing, the auditors have to possess expertise in the area of risk management as well as technical competence to audit algorithms. The recently adopted European Parliament position on the DSA adds extra safeguards to the original proposal. VLOPs have to allow auditors to access all necessary data, while auditors have to be financially and legally independent. Furthermore, the Parliament requires auditors and their employees not to provide any services to VLOPs 12 months before and after the audit is performed. Such safeguards could mitigate dangers that any independent private sector auditor could potentially face, as previously experienced with the GDPR auditing mechanism, i.e. corporate capture and inadequate independence. However, there is no guarantee that the Parliament's position will survive the pending trilogue negotiations.

In our view, the main weakness of this otherwise solid proposal lies in its enforcement. The DSA allocates strong enforcement powers to the European Commission over VLOPs. While a centralized enforcement model over Big Tech makes sense to some extent, monitoring compliance with criteria for independent audits or data access frameworks requires a specific set of technical skills. It also touches upon what body of the EU (if any) has that level of subject matter competence. Furthermore, the Commission is the executive branch of the EU and not exactly an independent regulator. To this day, it remains unclear what unit of the Commission will be assigned the role of enforcer. The following analysis will shed more light on the aforementioned issues while providing arguments in favor of creating a public sector auditing intermediary.

Institutionalizing a European public auditing intermediary

An auditing intermediary should serve several functions. First, it should verify and continuously audit whether the data provided by companies in mandatory transparency reports are credible and accurate (verification function). Second, it should facilitate transparency by lowering the costs of compliance for regulated companies and the costs of access for researchers, journalists, stakeholders, and the public (facilitation function). Third, it would allow for customization of access to data by tailoring it to individual needs thus reducing the need for unlimited disclosure of potentially sensitive and personal data, including by techniques such as differential privacy (tailoring function).

The verification service would be provided to regulators, civil society, journalism, academia, and the general public. By auditing public transparency reports provided by platforms as well as the submissions that are made to regulators within the context of specific legal frameworks such as the German NetzDG or the EU DSA before they are published by platforms. Beyond that, they could conceivably also audit any other claims made by online platforms and ensure that they are not – as is currently frequently the case – inaccurate or incomplete.

Second, the facilitation function is equally important. While with some large platforms gaming the numbers is a challenge, for many smaller providers it is difficult to provide meaningful transparency at a reasonable price. For many private sector organizations beyond the GAFAM, a public auditing intermediary who supports organizations in developing verifiable audited transparency in a standardized manner could also be a valuable service to reduce their existing compliance burden.

Third, the tailoring function of the auditing intermediary, for example, could ensure that the data researchers receive is accurate and appropriately redacted, for instance, due to compliance with the GDPR framework. Having an intermediary also reduces any potential risks for researchers and regulators, in that it avoids any danger of capture or data leakage on their part. The auditing intermediary could also implement differential privacy most effectively on a case-by-case basis, in a similar manner to the process being implemented by the U.S. census bureau.

The agency that will be entrusted with these three functions should be independent of authorities endowed with monitoring and sanctioning powers.

How should a European public auditing intermediary be organized?

None of the existing EU agencies is a perfect fit for the execution of the above intermediary auditing function. For all existing EU agencies that can be considered for this task, a substantial redesign of their mandate would be necessary. Among the EU institutions, there are three main candidates: the European Court of Auditors, the EU Fundamental Rights Agency, and the EU Joint Research Center.

The European Court of Auditors (ECA) has strong auditing capabilities but applies them mostly to the operation of public authorities. However, all public authorities are regularly audited for their spending and processes that also involve the purchasing or use of goods and services. ECA works with data, although in a very different form. The institution does not really offer actionable data sets, although it acts as a standardizing force in public finance auditing. From the perspective of the verification function, ECA seems like a natural candidate. However, its original mission is very distant from the goals of DSA and the meaningful transparency of private actors. ECA seems to have little experience and background to fulfill the facilitation and tailoring function.

The Fundamental Rights Agency of the European Union (EU FRA) has a strong legal and policy background, focusing on issues concerning information society and the protection of fundamental rights as prescribed by the EU Charter. However, it lacks any capabilities for the analysis of big data. Its expertise is mostly in legal research and socio-legal analysis. FRA has little experience with the analysis of company data and virtually no experience with offering raw big data sets to others. Therefore, while the mission of the agency is closer to the goals of the DSA, the agency seems to miss capabilities corresponding to all three functions that would be required to act as an auditing intermediary.

The Joint Research Center (JRC) is a scientific service of the European Commission. It produces research for EU policies. It is probably the closest organization in terms of analytical skills required for the auditing intermediaries. The employees are often researchers who have extensive experience with the study of market actors, various industries, and big data. The agency provides analytical inputs to institutions, and given the proximity to academic research, it also opens up its infrastructure, labs and data to others. The agency could therefore most easily perform the verification, facilitation, and tailoring function expected from an auditing intermediary.

However, JRC might be seen as insufficiently independent from the DSA enforcement part of the European Commission. JRC is currently organized as a DG under the responsibility of the Commissioner for Innovation, Research, Culture, Education and Youth (DG EAC). It is therefore separate, however, still part of the same overall institution. Giving it a role as an auditing intermediary would therefore require setting up clear principles of division.

Finally, there is also the possibility of creating a new independent European Platform Agency, as proposed and advocated for by the Greens/EFA political group in the European Parliament. However, the ‘super agency’ proposed by the Greens/EFA should be responsible for both enforcement and compliance oversight, with specific focus on VLOPs. We are not calling for a super agency of the kind proposed by the Greens, but could envisage a new EU agency acting as an auditing intermediary without additional regulatory powers beyond what is necessary for auditing platforms.

Europe needs independently verified platform data ASAP

The current lack of even basic reliable knowledge about online platforms should not be acceptable in democratic discourse. When only large online platforms, their staff and, occasionally, whistleblowers‘ testimonies are able to make reliable claims about what happens on key digital societal infrastructure, everyone suffers. This is not (just) a problem for citizens, journalists, academia, or civil society. Regulators and policy makers lack any reliable information about what actually happens on the platforms. Given a long history of inaccurate or misleading information provided by large online platforms, allowing platforms to continue to make unverified claims about their own systems cannot produce reliable outcomes. As societies, we have become epistemically impoverished by our inability to know what is happening on key digital societal infrastructure. Without basic knowledge of its own digital societal infrastructure, Europe cannot even begin to understand – let alone regulate – very large online platforms.