TU Delft

Delft University of Technology

Document Version
Final published version

Licence
Unspecified

Citation (APA)
Wagner, B., & Kuklis, L. (2021). Establishing Auditing Intermediaries to Verify Platform Data. In *Regulating Big Tech: Policy Responses to Digital Dominance* (pp. 169-179). Oxford University Press. https://doi.org/10.1093/oso/9780197616093.003.0010

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
In case the licence states “Dutch Copyright Act (Article 25fa)”, this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

Sharing and reuse
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.

9

Establishing Auditing Intermediaries to Verify Platform Data

BEN WAGNER AND LUBOS KUKLIS ■

INTRODUCTION

What you don't know can't hurt you: this seems to be the current approach for responding to disinformation by public regulators across the world. Nobody is able to say with any degree of certainty what is actually going on. This is in no small part because, at present, public regulators don't have the slightest idea how disinformation actually works in practice. We believe that there are very good reasons for the current state of affairs, which stem from a lack of verifiable data available to public institutions. If an election board or a media regulator wants to know what types of digital content are being shared in their jurisdiction, they have no effective mechanisms for finding this data or ensuring its veracity. While there are many other reasons why governments would want access to this kind of data, the phenomenon of disinformation provides a particularly salient example of the consequences of a lack of access to this data for ensuring free and fair elections and informed democratic participation.

This chapter will provide an overview of the main aspects of the problems associated with basing public regulatory decisions on unverified data, before sketching out some ideas of what a solution might look like. In order to do this, the chapter develops the concept of auditing intermediaries. After discussing which problems the concept of auditing intermediaries is designed to solve, it then discusses some of the main challenges associated with access to data, potential misuse of intermediaries, and the general lack of standards for the provision of data by large online platforms. In conclusion, the chapter suggests that there is an urgent need for an auditing mechanism to ensure the accuracy of transparency data provided by

large online platform providers about the content on their services. Transparency data that have been audited would be considered verified data in this context. Without such a transparency verification mechanism, existing public debate is based merely on a whim, and digital dominance is likely to only become more pronounced.

WHAT IS THE PROBLEM?

At present, public policy debates about online content are highly dependent on data provided by private sector organizations, almost always from a country outside their own jurisdiction. This problem is not just restricted to policy challenges associated with disinformation. It is clear that the need for accurate data transcends one particular regulatory area—be it media regulation, data protection, or telecommunications regulation.

For all of these areas, policymakers not only do not know how to resolve the policy issues at hand but also are unable to gain even a basic understanding of what the core problems associated with it might be. Private companies' voluntary provision of data in transparency reports is problematic not just because that data is unverified but also because their own presentation of categories and standards for transparency data allow them to shape the dimensions of the debate extensively. The way in which private sector platforms like Google or Facebook provide transparency reports under public disclosure requirements such as the German Network enforcement law or the EU General Data Protection Regulation is as a mechanism to manage the visibility of certain categories and obscure visibility from other categories (Flyverbom 2016; Albu and Flyverbom 2019).

Even in cases where transparency is mandated by law such as the German Network Enforcement Act (NetzDG), researchers and regulators alike have found the transparency data provided by Facebook to be highly problematic, with Facebook fined 2 million Euros for miscategorizing and misreporting data required in its government reporting requirements under the NetzDG (Wagner et al. 2020). This is due in part to Facebook prioritizing its own internal content moderation policy over external legal constraints systematically, but also to a lack of a joint industry standard by which data about content moderation is published. There is neither a standardized format provided by NetzDG that the resulting transparency data provided by either Facebook or any other online platform could be considered comparable. This lack of standardized reporting cannot just be blamed on states alone. It is equally due to the failure of large online platforms to standardize the manner in which they report their content moderation practices.[1]

Regulators and the general public are thus unable to make accurate determinations about what is happening in online platforms because they are currently unable to access accurate data about them. This limits both effective decision-making about the nature of existing policy problems policymakers are aware of,

as well as the ability to be able to respond to policy challenges they are not yet aware of.

In all of these contexts, the dominance of large transnational online platforms exacerbates this problem. Large platforms are more easily able to 'play' existing national jurisdictions against each other, for example, by threatening to switch the locations of their head offices if tangible regulatory burdens are increased. This was one of the key reasons why Tesla built their first European office in the Netherlands, and it seems a plausible way to explain the weak implementation of the EU data protection law GDPR by the Irish data protection authority. As one leading international election observer noted, 'we're running after the tech companies, they have enormous resources, and they're playing us' (Wagner 2020). The dominance of large online platforms also contributes to limiting the ability of any one regulatory jurisdiction to gain access to relevant data.

WHAT COULD BE THE SOLUTION?

From the perspective of the authors, the most helpful response would be to develop an institutionalized mechanism for the verification of platform data. This would ensure that the data public regulators receive is accurate and verified. At the same time, if all regulators were given competences and capacities to verify data important for the exercise of their duties individually, it would create considerable redundancies. These redundancies may not only be inefficient economically but could also cause complicated situations potentially leading to mishandling of the data itself. As such, a separate institutionalized mechanism which provides a verification function for data provided by platforms to regulators would be the most effective response to this problem. In this context, verified data is understood as verified data provided as part of transparency reports by platforms or similar public disclosures. Independent auditors have checked this data to ensure it is an accurate representation of the state of the platform.

Importantly, gaining access to relevant data does not mean access to all data at all times by all regulators. This article should not be misunderstood as an argument for the creation of NSA-Style 'direct access' to online platforms by any regulator who wishes to respond to a policy problem. Rather, there is a clear need for verified data that answers specific policy questions that regulators have, as well as for existing regular reporting requirements. Providing any government regulatory agency with unlimited access to a dominant online platform is highly problematic and only serves to increase existing challenges around digital dominance. Giving public sector actors unfettered access to dominant online platforms does not reduce the problem of digital dominance.

There are some notable exceptions to this, in particular in the context of platforms hosted by more authoritarian governments. It seems plausible that the government of China has direct access to relevant data on large online platforms such as Sina Weibo, TikTok, or WeChat (Wagner 2012; Jiang and Fu 2018; Jiang 2019; Kloet et al. 2019; Hong and Harwit 2020). Indeed, the Chinese

government's ability to correct what they consider disinformation on these platforms in near real-time and heavily influence platform developments in the area of content moderation suggest a great deal of access to data and a close relationship between government regulators and large online platforms. It seems unlikely that government regulators in a situation like this would have concerns with being provided inaccurate or incomplete data. However this highly authoritarian solution is not a plausible solution for democratic governments, it is not possible to safeguard key human rights such as freedom of expression or privacy while also enabled unfettered access to what the citizens of democratic governments do online.

It can even be argued in this context that the existing lack of access and accountability in the area of online platforms makes authoritarian approaches to the governance of the Internet more likely. National regulators unable to access accurate data from dominant online platforms are left with few good policy options. This is particularly the case when the unchecked power of these platforms has the ability to influence elections or other key democratic goods. Rather than strengthen the authoritarian impulses of states across the world, there is an urgent need for models of government that enable an approach that allows for greater accountability of the power of dominant online platforms. The first step in order to achieve this is providing access to accurate and verified data.

Auditing Intermediaries

Within this context, the appropriate institutional accountability mechanism (Bovens 2010) to ensure the accuracy of data provided by online platforms is to create an auditing intermediary—public or private sector entity, that audits data provided by large online platforms upon request. Doing so would resolve a variety of problems associated with privacy, scope, security, redundancy, capacity, and institutional capture within the auditing process.

First, by bundling the auditing process through centralized auditing intermediaries, it limits the exposure of sensitive private data to as few actors as possible. Privacy and data protection are central concerns for organizations that wish to provide transparency, with existing privacy laws such as the GDPR limiting mechanisms disclosure (Bankston 2018; Keller 2018). Using auditing intermediaries limits challenges associated with privacy and data protection, as it can ensure that a more limited subset of verified data is provided to both regulators and the general public. It also follows the principle of data minimization, which is enshrined in Article 5 of the GDPR.

Second, by distancing the audit process from the regulator that is asking for data, it ensures that regulatory action does not overstep its bounds (Viscusi 1996; Hodge 2015). Particularly given the diversity of regulators with an interest in regulating online platforms and the considerable power which can be drawn from access to their data, ensuring that regulators remain within the scope of their mandate is particularly important (Becker 2013; Yan 2018).

Third, by limiting the number of points through which the online platforms need to interact with outside intermediaries, it limits potential security risks that could arise from providing a broad set of different regulators access to a wide variety of systems. It is to be assumed that any kind of access provided to data by large online platforms is highly likely to constitute a considerable security risk. As a result, limiting the number of individuals with access limits the potential exposure to this specific risk.

Fourth, having numerous regulators involved in auditing is likely to create numerous unnecessary and redundant processes in which similar regulators ask similar questions which need to be answered separately over and over again. This challenge is not dissimilar to regulating government surveillance practices (Korff et al. 2017), where ensuring effective oversight depends heavily on ensuring that online platforms are not able to provide conflicting answers to a set of broadly similar questions. At the same time, centralizing the answers provided through a central point avoids redundancy and strengthens the coherence of the overall argument being made.

Fifth, organizing auditing of transparency data through an external auditing intermediary ensures that even regulators without the capacity to organize audits themselves still may have access to such a system through auditing intermediaries. Even existing European regulation like the GPDR is posing considerable challenges in regard to enforcement, with key regulators like the Irish Data protection authority seen as lacking the capacity to do so effectively (Scally 2020). This challenge is even more the case in jurisdictions which are less developed and have fewer resources to invest in regulation as a result. However, it is precisely these jurisdictions where regulatory support is most needed. The ability to regulate a large online platform should not be limited to the largest and most powerful regulators.

Sixth, there is an ongoing interchange of staff between media regulators and those being regulated, which brings with it the risk of institutional capture of the regulators (Nielsen et al. 2019; Short 2019). This risk is even more pronounced in regard to auditing intermediaries, as a result of their potential access to particularly sensitive material. A staff member of an auditing intermediary could not audit Facebook and then work for Google six months or even several years later. As these kinds of restrictions are particularly onerous and limit the recruitment of staff, they should be limited to a small group of auditors rather than a wider regulatory body, although they are of course desirable for regulators as well. As such, the creation of an auditing intermediary brings considerable benefits with it, but what would it look like in practice?

Public or Private Auditing Intermediaries?

The most important question about an auditing intermediary is the question of whether such an intermediary would be public, private or somewhere in between. While both are legitimate approaches to the challenge of auditing intermediaries,

due to limited space this chapter only develops the approach of a public intermediary further here. What could such an independent public intermediary look like?

The first and most important is that any such public intermediary would need to be highly independent. This has been a challenge in previous iterations of public sector platform regulation, which is part of why an independent agency—preferably at a European level—would be of such high importance. For example, the German 'Bundesamt für Justiz' (BfJ) is entrusted with enforcing the German Network Enforcement Act (NetzDG) which is, in turn, one of the key current elements of platform regulation in Europe. However, the BfJ is not an independent regulator, rather it is directly attached to the German Ministry of Justice and has to follow the instructions of the Ministry and the politically appointed Minister of Justice (Wagner et al. 2020). As such, a public agency similar to the BfJ would not be in a position to conduct this kind of verification.

We thus believe that it is important to create a new institution that draws on auditing expertise in the private and public sectors to verify the claims made by social media providers. One stage removed are media and other regulators, who are themselves independent agencies within the national context. The extent of their independence, however, varies to a considerable degree. And even those that can be considered sufficiently independent are usually not equipped with the capacities or competencies for auditing data. Although not inconceivable, it would require a substantial restructuring of these institutions in every member state to allow for such an activity.

Finally, there is the case of data protection authorities (DPAs), which are also independent agencies. Through their experience and expertise with data protection impact assessments under the GDPR and their in-house technical skills, they would be well-equipped to conduct these kinds of audits. However, they are already significantly understaffed and underfunded to respond to the GDPR, without having additional burdens for additional tasks placed upon them. Importantly, their role as DPAs in ensuring the compliance with data protection rules and regulations is very different than auditing the accuracy of transparency reports.

Such an institution could be created within the context of the proposed European Digital Services Act (DSA). It should, however, be a distinct legal entity to safeguard its independence from other institutional actors working in this area. The ability to draw on expertise from the European Court of Auditors, from the European Data Protection Supervisor (EDPS), as well as from the private sector would be essential to enable the effective functioning of this institution.

This institution would be responsible for collecting verified data and making them available only to authorities endowed with the legal competence to use them, to a legally specified extent for a legally-specified purpose. The collection and verification of the data on the one hand, and their use for regulatory purposes on the other, would, therefore, be distinct processes, which would further enhance the independence of the institutions involved, and the security of the data in question.

WHAT CHALLENGES DOES THE CREATION OF AN AUDITING INTERMEDIARY CREATE?

The proposal of auditing intermediaries brings with it its own set of challenges. The following section briefly provides an overview of what these difficulties are and how some of these difficulties might be overcome.

How Much Access Do Auditing Intermediaries Need?

One of the key challenges raised by the proposal of auditing intermediaries is how much access to data these intermediaries would actually need. It is, of course, easy to raise privacy concerns in this context. After all, who wouldn't be concerned about a government regulator having access to all the digital content they are sharing? Public regulators do not need access to all digital content to combat disinformation or to respond to problematic online content or hate speech. Nor do they—as some policy proposals have suggested—need to 'break encryption' or mandate unencrypted communications on key platforms in order to be able to conduct it effectively.

Instead, like any other similar auditor from the financial sector, they would need access to some relevant data about the platform, the infrastructure behind it, and the existing policies in place. This is similar to the way in which the compliance with anti–money laundering (AML) rules is monitored in the financial sector. Banks in the United States are required under existing US AML legislation to monitor certain types of transactions and submit suspicious activity reports to the Financial Crimes Enforcement Network (Naheem 2015). When compliance with money laundering legislation is audited, auditors are not interested in looking at each individual transaction or document received by the bank, but rather at the procedures and mechanisms that have been put in place to produce these results (Naheem 2016). The analogy can thus be drawn that auditing the processes and procedures in place to produce reporting is likely to be much more effective than providing access to all pieces of data. Thus, auditing mechanisms do not have to include personal data of any individuals. An understanding of the procedures around how personal data is processed, managed, and governed is likely to be far more important. Being able to reproduce and spot check that the transparency reports are being produced accurately represent the data governance practices of the individual platform is critical to any meaningful audit.

Misuse of Auditing Intermediaries for Strategic National Interests

Even without any kind of direct access, auditing intermediaries remain an important locus of power. Given their ability to gain some degree of access to the

dominant online platforms they are auditing, they will quickly become the focus of struggles for power. While this is evidently already the case within powerful online platforms themselves (Moore and Tambini 2018), auditing intermediaries are likely to be in a similar situation. Thus, they need to be adequately shielded from these power struggles by guaranteeing their institutional independence and ensuring their staff selection and maintenance procedure is beyond reproach. Without meaningful protection, auditing intermediaries would quickly lose their credibility as impartial auditors (Funnell et al. 2016; Gipper et al. 2019). This is why it is so important to safeguard their independence and ensure effective staff selection and maintenance procedures.

Standard Setting for Online Platform Transparency Reports

Finally, one of the most significant challenges is that common standards for the provision of data in transparency reports or indeed for different types of regulatory requests currently do not exist. Each company publishes its own data and each regulator makes requests in its own format. This lack of standardization and structure in reporting requirements makes it highly challenging for regulators, the general public, academics, and dominant online platforms alike. As each platform has developed an 'organic structure' for responses to regulatory compliance, the meaning of platform responses to these requests is far from clear, let alone comparable.

At the same time, standard setting for transparency reports takes place primarily through individual legislative acts for specific sectors or policy domains. There is no linkage for the reporting standards for privacy under the GDPR and for German the Network Enforcement Law (NetzDG), nor any attempt to coordinate or structure them in a systematic way. This leads to challenges as the systems of the platforms are not providing comparable data because the infrastructure that they have in place was not designed to collect it in such a manner. This challenge of structuring access to data is similar to government requests for additional passenger data from airlines (Hasbrouck 2020). Typically, the ways in which data is requested from online platforms and airlines alike assume common system and reporting mechanisms that allow for a systematic and standardized response. In doing so, they ignore the considerable time and investment required to ensure reporting is possible in a systematic and standardized manner.

Of course, all of this energy would not have to be expended if large online platforms had already, through an industry group, trade body, or similar structure, come up with their own joint standards for managing and governing content on their platforms. For the airline industry, three airlines associations WCO/IATA/ICAO got together, and in their joint 'API Contact Committee' developed a standardized format and protocol called PNRGOV.[2] As such standards are lacking, there is a need for public sector actors to step in and define these standards themselves. Ideally, by standardizing compliance requirements systematically, this

would enable a common regulatory framework that allows regulators to make requests of online platforms without constantly reinventing the wheel.

CONCLUSION

Current transparency data provided by online platforms does not stand up to rigorous scrutiny, either by independent academics, media regulators, or civil society. In the same way that the financial services regulator relies on 'auditing intermediaries' to ensure the accuracy and veracity of the annual reports of companies, so too should media regulators and election boards be able to rely on auditing intermediaries to ensure that the data they receive is accurate. In which other industry would it be considered reasonable to take the claims of a private company about key financial aspects of its business on face value without independent verification? If we can expect this level of audited scrutiny for financial transactions, why not also for digital content?

This chapter has shown several other examples from other areas, most notably the financial services and aviation, where elements of relevant mechanisms exist. Although there is no need to reinvent the wheel, the extraordinarily dominant power of large online platforms requires even higher standards of transparency, accountability, and good governance, if auditing intermediaries are to be successful. We believe that this chapter has shown that it is possible to develop auditing intermediaries and that there are many strong reasons to do so.

Importantly, a regulator of this kind can strengthen freedom of expression rather than impeding it. Freedom of expression is the right to seek, receive, and impart information, even if it is frequently reduced to being able to say whatever you want without facing any consequences for doing so. Auditing intermediaries can strengthen the right to seek and receive information, by making sure that users are completely and accurately aware of how the content on large platforms is governed. Ensuring greater transparency of online platforms means users will know why some content was removed, why other content stayed up, or why platform algorithms show certain types of content and not others. This contextual information is crucial to being able to exercise freedom of expression rights. Without it, users have to rely on statements made by the large online platform without any verification or validation of the underlying data. By doing so, auditing intermediaries can contribute to stopping the spiral of privatization of the governance of freedom of expression, making it more transparent and accountable towards users and the public at large (Wagner 2011, 2018).

What is not possible, at this point, is to continue public debates or regulatory policy about the actions of large online platforms based on unverified data. Only if regulators have an accurate picture of what is actually happening on large online platforms, whether regarding disinformation or numerous other public policy issues, can they make accurate determinations of what steps to take. Neither regulators nor the general public should have to rely on the benevolence of online platforms to know what is going on in their own media environments.

NOTES

1. See, for example, https://rankingdigitalrights.org/.
2. See https://media.iata.org/iata/passenger-data-toolkit/library.html for further details.

REFERENCES

Albu, O. B., and M. Flyverbom. 2019. 'Organizational Transparency: Conceptualizations, Conditions, and Consequences'. *Business & Society* 58: 268–97.

Bankston, K. 2018. 'How We Can "Free" Our Facebook Friends'. *New America Foundation*.

Becker, L. 2013. 'Accountability Gets Personal'. *Risk* 26: 28–29.

Bovens, M. 2010. 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism'. *West European Politics* 33: 946–67.

Flyverbom, M. 2016. 'Digital Age Transparency: Mediation and the Management of Visibilities'. *International Journal of Communication* 10: 13.

Funnell, W., M. Wade, and R. Jupe. 2016. 'Stakeholder Perceptions of Performance Audit Credibility'. *Accounting and Business Research* 46: 601–19.

Gipper, B., C. Leuz, and M. Maffett. 2019. 'Public Oversight and Reporting Credibility: Evidence from the PCAOB Audit Inspection Regime'. The Review of Financial Studies, 1–148.

Hasbrouck, E. 2020. 'Airline Passenger Data and COVID-19'. https://papersplease.org/wp/2020/04/06/airline-passenger-data-and-covid-19/

Hodge, N. 2015. 'Overstepping Their Authority: As Regulatory Actions Increase, Organizations Are Finding That Regulators Can Be Overzealous in Their Pursuit of Justice'. *Risk Management* 62: 28–33.

Hong, Y., and E. Harwit. 2020. 'China's Globalizing Internet: History, Power, and Governance'. *Chinese Journal of Communication* 13: 1–7.

Jiang, M. 'Cybersecurity Policies in China'. CyberBRICS: Mapping Cybersecurity Frameworks in the BRICS. 2019.

Jiang, M., and K.-W. Fu. 2018. 'Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?' *Policy & Internet* 10: 372–92.

Keller, D. 2018. 'Comments on the Guidelines on Transparency under Regulation 2016/679'. Rochester, NY: Social Science Research Network.

Kloet, J. de, T. Poell, Z. Guohua, et al. 2019. 'The Platformization of Chinese Society: Infrastructure, Governance, and Practice'. *Chinese Journal of Communication* 12: 249–56.

Korff, D., B. Wagner, J. Powles, et al. 2017. 'Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes'. Rochester, NY: Social Science Research Network.

Moore, M., and D. Tambini. 2018. *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*. New York, USA: Oxford University Press.

Naheem, M. A. 2015. 'HSBC Swiss Bank Accounts—AML Compliance and Money Laundering Implications'. *Journal of Financial Regulation and Compliance* 23: 285–97.

Naheem, M. A. 2016. 'Money Laundering: A Primer for Banking Staff'. *International Journal of Disclosure and Governance*13: 135–56.

Nielsen, R. K., R. Gorwa, and M. de Cock Buning. 2019. 'What Can Be Done? Digital Media Policy Options for Europe (and Beyond)'. Reuters Institute for the Study of Journalism, Oxford.

Scally, D. 2020. 'German Regulator Says Irish Data Protection Commission is Being "Overwhelmed" '. *Irish Times*, Feb 3, 2020.

Short, J. L. 2019. 'The Politics of Regulatory Enforcement and Compliance: Theorizing and Operationalizing Political Influences'. *Regulation & Governance*, 1–33. https://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12291

Viscusi, W. K. 1996. 'Regulating the Regulators'. *The University of Chicago Law Review*: 63(4): 1423–61.

Wagner, B. 2011. 'Freedom of Expression on the Internet: Implications for Foreign Policy'. *Global Information Society Watch* : 18–20.

Wagner, B. 2012. *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy*. Brussels, Belgium: European Union.

Wagner, B. 2018. 'Free Expression?—Dominant Information Intermediaries as Arbiters of Internet Speech'. In *Digital Dominance*: *The Power of Google, Amazon, Facebook and Apple*, edited by M. Moore and D. Tambini. Oxford: Oxford University Press. Pp. 219–240.

Wagner, B. 2020. 'Digital Election Observation: Regulatory Challenges around Legal Online Content'. *Political Quarterly 91*: 1–6.

Wagner, B., K. Rozgonyi, M.-T. Sekwenz, et al. 2020. 'Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act'. Barcelona, Spain: ACM Conference on Fairness Accountability and Transparency (FAT* 2020).

Yan, X. 2018. 'The Jurisdictional Delimitation in the Chinese Anti-Monopoly Law Public Enforcement Regime: The Inevitable Overstepping of Authority and the Implications'. *Journal of Antitrust Enforcement* 6: 123–49.