Closing information gaps in DMA enforcement—expectations, incentives, and the role of anonymity for whistleblowers

Sarah Hinck, Jasper van den Boom

Article - Version of Record

Suggested Citation:
Hinck, S., & van den Boom, J. (2025). Closing information gaps in DMA enforcement—expectations, incentives, and the role of anonymity for whistleblowers. Journal of Antitrust Enforcement, 2025(00), Article jnaf017. https://doi.org/10.1093/jaenfo/jnaf017

Journal of Antitrust Enforcement, 2025, **00**, 1–23
https://doi.org/10.1093/jaenfo/jnaf017
Article

Closing information gaps in DMA enforcement—expectations, incentives, and the role of anonymity for whistleblowers

Sarah Hinck[1,*], Jasper van den Boom [1]

[1]Shaping Competition in the Digital Age (SCiDA), Chair for Civil Law, German and European Competition Law, Heinrich Heine University, Düsseldorf, 40225, Germany

*Corresponding author. PhD Researcher, Heinrich Heine University, Universitätsstr. 1, 40225 Düsseldorf, Germany. E-mail: Sarah.hinck@hhu.de

ABSTRACT

The introduction of the Digital Markets Act (DMA) Whistleblower Tool marks an important step in encouraging informants to report DMA breaches by gatekeepers, while navigating the complexities of anonymity and protection for informants. This article aims to answer the question of how the implementation of the DMA Whistleblower Tool impacts potential whistleblowers and their incentives to come forward. To this extent, we examine varying levels of anonymity (full, partial, non-anonymous) and their respective advantages and disadvantages for whistleblowers, highlighting the necessity for regulators to secure protections against retaliation without compromising administrative efficiency or due process. Despite the DMA's intention to apply the protections of the Whistleblower Directive (WBD), practical implementation has lagged, creating several challenges. The DMA's reliance on the WBD faces obstacles due to the decentralized nature of the WBD, the DMA's centralized reporting system, the differing focus of internal versus external reporting channels, and the mismatch between the WBD's focus on insiders and the DMA's broader range of potential informants, such as business users and competitors. These issues point to the need for enhanced procedural clarity, better utilization of national competition authorities, improved alignment between the DMA and the WBD, and the formation of DMA interest groups to advocate for business users.

KEYWORDS: Whistleblowers; Digital Markets Act; gatekeepers; business users; third-party rights
JEL CLASSIFICATIONS: K20, K21, K23, L43

1. INTRODUCTION

The Digital Markets Act (DMA)[1] requires the European Commission to monitor and enforce compliance by designated gatekeepers with the obligations set out in the law. Where Big Tech ecosystems dominate digital platform markets, effective compliance with the DMA shall ensure contestability and fairness in these markets. This requires the Commission to monitor a large number of compliance measures, while facing hurdles such as limited access to resources and significant information asymmetries between the regulator and the regulated firm.[2] Whistleblowers could therefore play a key role in gathering insider information about certain behaviour or processes. In the context of the DMA, business users are likely best placed to explain to the Commission why certain compliance mechanisms work or do not work.[3] After all, business users depend on the chosen compliance measures and have the greatest interest in solutions that work.[4] Furthermore, where the gatekeeper platform plays a dual role (ie as platform operator and as competitor in downstream markets), business users have first-hand experience of how self-preferencing by gatekeepers can affect competition in these markets.[5] At the same time, these business users find themselves heavily dependent on the platform operator.[6] This can make them very reluctant to come forward: being disintermediated can lead to a significant loss of revenue or even foreclosure. Both the risk of retaliation and the potential damage associated with retaliation were illustrated by Apple's decision to ban Epic Games from its App Store, a decision that was seen as retaliation for Epic's active cooperation with enforcement authorities and its litigation against Apple.[7]

Against this background, the European Commission launched its DMA Whistleblower Tool on 30 April 2024.[8] This tool is the first official communication channel for third parties and is intended to facilitate anonymous or non-anonymous submissions by insiders. In this way, the tool aims to assist the Commission in gathering information to open cases and to collect evidence to support its investigations under the DMA against gatekeepers. Outside of the DMA Whistleblower Tool, the procedural design of the DMA does not provide for any relevant rights of participation for third parties beyond the provision of information to the Commission. This is a clear departure from European Union (EU) competition law, where procedural rights for third parties are far more established.[9]

Rather than strengthening formal third-party participation in DMA proceedings, the DMA Whistleblower Tool should therefore be seen in the context of the legislative decision to extend the scope of the Whistleblower Directive (WBD)[10] to the DMA. The Directive was introduced in 2019 after a number of high-profile whistleblowing cases, such as those of WikiLeaks's Julian Assange or Meta's Francis Haugen, sparked a debate on the appropriate

[1] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[2] G Monti, 'The Digital Markets Act: Improving its Institutional Design' (2021) *CoRe* 2 92.

[3] ibid, 101.

[4] A De Streel, 'DMA Implementation Principles' in A De Streel and others (eds), *Implementing the DMA: Substantive and Procedural Principles* (CERRE 2024) 11.

[5] Case C-48/22 *P—Google and Alphabet v Commission* [2024] EU:C:2024:726 (Google Shopping).

[6] This dependency is recognized in Rec 2, 20, 40 Digital Markets Act.

[7] M Acton, 'EU Probes Apple Over App Store Shutdown of Epic Games' *Financial Times* (7 March 2024); CREATe, 'The Apple-Epic Saga and the Digital Markets Act' (*CREATe Blog*, 28 March 2024) (online).

[8] European Commission, *Commission Launches Whistleblower Tools for Digital Services Act and Digital Markets Act*, press release, 20 April 2024, online.

[9] W Wils, 'Procedural Rights and Obligations of Third Parties in Antitrust Investigations and Proceedings by the European Commission' (2022) Concurrences (online).

[10] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (Whistleblower Directive).

level of protection for whistleblowers.[11] The WBD establishes a system of protection for whistleblowers to encourage individuals to come forward with inside information about possible breaches of EU law. This protection is, however, focused on *insiders* who want to come forward with sensitive information; it has not been designed to protect the identity and rights of *business users* in mind.

The introduction of the DMA Whistleblower Tool in the context of otherwise limited procedural rights of third parties in DMA procedures, and the application of the WBD protection regime to the DMA to incentivize third parties to come forward while protecting them from retaliation by gatekeepers, raises a number of questions. First, it prompts reflection on the importance of anonymity in procedures involving power asymmetries. Secondly, the alignment between the requirements of the WBD, which is directed at Member States and focused on the protection of individuals, and the legislative and enforcement design of the DMA seems questionable. The ambiguity surrounding the protections offered under the DMA, as well as the lack of procedural rights, may limit incentives to come forward. Third, the introduction of the DMA Whistleblower Tool raises the question of further measures to ensure that the Commission receives relevant information on DMA violations while preventing retaliation against business users and keeping procedures streamlined.

On the basis of the conceptual and practical issues identified, the article assesses the implementation of the objective of incentivizing and protecting whistleblowers in relation to DMA violations. Section 2 discusses the value of information provided by third parties and the costs and benefits associated with parties coming forward with varying degrees of anonymity. Section 3 of the article analyses the role and protection of whistleblowers under the DMA. It does so by assessing the background and scope of the WBD, its relationship to the DMA, including the design of the DMA Whistleblower Tool, and how this affects incentives to come forward. The article identifies a number of shortcomings of the DMA and its DMA Whistleblower Tool in relation to the requirements of the WBD and the role of third parties under EU competition law. In Section 4, the article suggests some ways forward to improve the position and incentives of whistleblowers to provide information on potential violations of the DMA.

2. SYSTEMIZING ANONYMITY: FULL-, PARTIAL-, AND NON-ANONYMOUS INFORMATION

Inside information is often crucial to law enforcement. Where the risk of retaliation is particularly high, for example in criminal proceedings, legal regimes provide options to provide information anonymously or in confidence.[12] However, maintaining anonymity or confidentiality throughout proceedings has a number of implications for the different stakeholders involved. To some extent, these implications depend on the degree of anonymity or confidentiality to protect the identity of the informant versus full disclosure.

In order to ensure consistent taxonomy throughout the article, the subsection briefly discusses the conceptual differences between information provided fully anonymously, partially anonymously (ie with an agreement to keep the identity confidential), and non-anonymously. To provide a nuanced approach to the value and desirability of anonymous information in law enforcement in general, and in DMA enforcement in particular, the

[11] See, eg, LM Sifrey, *A Tale of Two Whistleblowers: Daniel Ellsberg, Frances Haugen and the Fight for the Truth* (Substack 20 June 2023) (online).

[12] N Combs, 'Witness Protection, in The Challenge of Witness Protection' in Sharon Weill and other (eds), *The President on Trial: Prosecuting Hissène Habré* (Oxford University Press 2020) 381; S Lonati, 'Anonymous Witness Evidence before the European Court of Human Rights: Is It Still Possible to Speak of "Fair Trial"?' (2018) European Criminal Law Review 120.

'Benefits and drawbacks of different levels of anonymity' section also highlights some of the advantages and disadvantages associated with different levels of anonymity.

The distinction between full, partial, and non-anonymity

Disclosure of the identity of informants, witnesses, or parties to proceedings can be considered the general rule in law enforcement procedures as the right of confrontation is part of the right of defence guaranteed by Article 6 of the European Convention on Human Rights, and Article 41 of the Charter of Fundamental Rights.[13] However, in exceptional circumstances, in particular where there is a real risk of retaliation, an exception may be made to allow informants to come forward without revealing their identity to the accused. To this end, legal regimes provide various mechanisms to protect the identity of informants. While these mechanisms differ in the level of protection provided, the nomenclature used for anonymity or confidentiality in this context also differs.

While anonymity for informants is provided for in a number of EU laws, including competition law,[14] there is no single definition at the EU level.[15] Instead, anonymity is often defined at the Member State level. Even there, the exact definition of anonymity is often debated and open to national interpretations.[16] One definition related to anonymity at the EU level appears in Recital 26 of the General Data Protection Regulation (GDPR) and serves as a starting point for understanding anonymity in the EU context.[17] This recital defines anonymous information as information that 'does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'. Thus, in the GDPR, anonymity is used to refer to data subjects who have either never been identified, or where the data subject is unidentifiable following a process of pseudonymization.[18] Both parts of the GDPR's definition protect a subject's identity. However, the first part aligns with what is described here as full anonymity. The second part is closer to the concept of partial anonymity or confidentiality.

An informant is *fully anonymous* if his or her identity has not been disclosed to anyone, including the enforcement authority, the judge, or even the legal counsel.[19] An informant is *partially anonymous* if the identity of the informant is known to the relevant authority, but is kept confidential from any outside party (for instance, through pseudonymization), unless exceptions apply. The degree of confidentiality may vary. For example, in some cases, the identity may be shared between the notified authority and other authorities or courts,

[13] ibid 120–122.

[14] This possibility was first established in case law, See Wils (n 9) in reference to Judgments of 7 November 1985, *Adams v European Commission*, 145/83, EU:C:1985:448, para 34; of 8 July 2004, *Mannesmannröhren-Werke v Commission*, T44/00, EU:T:2004:218, para 84, confirmed on appeal in Judgment of 25 January 2007, *Salzgitter Mannesmann v European Commission*, C411/04 P, EU:C:2007:54, para 45; of 8 July 2004, *Dalmine v European Commission*, T50/00, EU:T:2004:220, para 72, confirmed on appeal in Judgment of 25 January 2007, *Dalmine v European Commission*, C407/04 P, EU:C:2007:53, para 49; and of 8 July 2008, *BPB v European Commission*, T53/03, EU:T:2008:254, para 36. The confidential treatment of the identity of complainants is later recognized in the European Commission's antitrust manual, see European Commission (2019), ch 12 'Access to file and Confidentiality', para 30. It is also codified through Regulation 773/2004, where it can be viewed as a category of other confidential information.

[15] See Rec. 20 Directive 2019/29/EU (Victim's Rights Directive); art 24(5) Regulation 2016/794 (Europol Regulation); Reg 23 Dir 2009/52/EC, art 30(2) Regulation 2017/1939.

[16] S Van der Hof, B-J Koops and RE Leenes, 'Anonymity and the Law in the Netherlands' in I Kerr, V Steeves and C Lucock (eds), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, (Oxford University Press 2009) 503–521.

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[18] B Van der Sloot, S Van Schendel and CA Fontanillo López, 'The Influence of (technical) Developments on the Concept of Personal Data in Relation to the GDPR' Report for the WODC (2023) 132.

[19] Lonati (n 12) 122.

whereas in other cases, the identity is only disclosed to the notified authority. The Commission's whistleblower tools, for example, foresee options for both fully anonymous and partially anonymous complaints. However, the quality of the information provided and the ability of the Commission to verify the claims will impact the likelihood that it starts an investigation.[20]

Benefits and drawbacks of different levels of anonymity

The benefits and drawbacks associated with different levels of anonymity arise from an important trade-off between trusting information from an undisclosed source, the increased administrative burden of protecting identities, and the procedural rights of defence involved. In the context of law enforcement, each party involved—the enforcer, the informant, and the defendant—benefits differently from anonymous, confidential, or non-anonymous information.

For fully anonymous information, there are three main benefits. First, the high level of protection of full anonymity in proceedings ensures the lowest barriers to coming forward. For the informant, the risk of retaliation is significantly reduced.[21] Secondly, from an enforcement perspective, by increasing the likelihood of coming forward, full anonymity can increase the likelihood of preventing, uncovering, and penalizing wrongdoing. Thirdly, full anonymity is a relatively low-cost measure to protect whistleblowers.[22] As long as the identity of the whistleblower remains unknown, the authority does not need to take additional measures to prevent or penalize retaliatory measures.[23]

The drawbacks of completely anonymous information reflect the benefits of full disclosure of the identity of the informant. Anonymity in proceedings limits or even violates, the right to confrontation, and possibly the right to a fair trial.[24] If the accused does not know his or her accuser, it is harder to develop a defence. From the enforcer's point of view, the authority would have to justify why it considers the anonymous information to be relevant and reliable, which will be difficult to verify in the case of a completely anonymous informant.[25] For the informant, full anonymity limits the rewards for coming forward. These may include enhanced procedural rights, leniency, or compensation for the damages caused by the defendant's conduct.[26] Moreover, if the anonymous complainant fails to provide sufficient information for the Commission to verify their claims, it will not lead to an

[20] European Commission, *Report a Breach of EU Law by an EU Country* (2024) (online).

[21] A Beijer, AM Hoorn, 'Netherlands Reports to the Fifteenth International Congress of Comparative' Conference Report (1998) 523–548 describe how anonymous witness complaints became relevant as one method for the protection of witnesses.

[22] Leonardo Labriola, 'Paying Too Dearly for a Whistle: Properly Protecting Internal Whistleblowers' (2017) 85 Fordham Law Review 2839, 2846.

[23] TM Marcum and J Young, 'Blowing the Whistle in the Digital Age: Are You Really Anonymous? The Perils and Pitfalls of Anonymity in Whistleblowing Law' (2019) 17 Depaul Business and Commercial Law Journal 1 explains that this does require the whistleblower to actually remain anonymous. It is easy to leave digital traces of one's identity, which still creates a risk of exposure.

[24] See Lonati (n 12) 122 states that 'Albeit not expressly acknowledged in Article 6 of the Convention, the interests of witnesses and victims of crimes against life, security, and freedom, are protected by other provisions of the Convention and may not be ignored.' In this regard, the European judges have noted: 'It is true that Article 6 does not explicitly require the interests of witnesses in general, and those of victims called upon to testify in particular, to be taken into consideration. However, their life, liberty or security of person may be at stake, as may interests coming generally within the ambit of Article 8 of the Convention', in reference to Van Mechelen and others v. The Netherlands, Application no 21363/93, Judgment 23 April 1997, margin no 54; RW Kirst, 'Hearsay and the Right of Confrontation in the European Court of Human Rights' (2003) 21 Quinnipiac Law Review 777.

[25] Recent case law by the Court of European Human Rights has provided a number of reasons as to why the use of anonymous witnesses must be justified, and when it is considered impermissible, at least in the context of criminal cases, see *Vasilyev and others v Russia* 22 September 2020 (Application no 38891/08). Here, the Court explains that even if the witness can be heard with a distortion of voice and while hiding one's appearance, there are still significant barriers to verifying the statements of witnesses as their identity is unknown, and opportunities for cross-examination are limited.

[26] See eg Wils (n 9), OECD (2023).

investigation.[27] At the same time, providing too much unique information for the purpose of verification may reveal the complainant's identity.[28]

Some of these issues may be mitigated by partial anonymity, that is by disclosing the identity of the informant only to the enforcer. This allows the latter to better verify the reliability of the information, and to justify the use of this information. However, some drawbacks remain. The defendant's rights of confrontation are still limited, and sensitive information can still be withheld.[29] If certain information is redacted to protect the identity of the informant, this is tantamount to limiting the defendant's access to the file.[30] Disclosure of identity also increases the risk of (accidental) identification. The enforcer thus faces an increased administrative burden to protect the identity of the informant by establishing procedures and protocols to prevent incidents or leaks.[31]

Whether a departure from the basic rule that informants should be identifiable (non-anonymous), where there is little or no risk of retaliation,[32] is justified ultimately depends on the facts and circumstances of the case.[33] Allowing anonymity in proceedings, therefore, always requires a balancing of interests and potential trade-offs for the stakeholders involved.

3. WHISTLEBLOWING IN THE DMA

Whistleblowers—be they insiders or stakeholders—are a valuable source of information. While the role of third parties in identifying non-compliance is recognized in both competition law and the WBD, the procedural role of third parties under the DMA itself is limited. This may be due to the expected self-executing nature of the DMA and the legislative intent to expedite proceedings. After all, allowing third parties to intervene in procedures tends to make them longer, rather than shorter.[34] Nevertheless, there must be ways for stakeholders, especially business users of digital platforms, to approach the Commission and request enforcement. The objective of the DMA is to "ensure contestability and fairness for digital markets in general, and *for business users and end users*" (emphasis added) of gatekeepers.[35] The DMA thus seeks to regulate the power asymmetries of gatekeepers vis-à-vis their users. Information from these users, who are at the same time highly dependent on digital platforms, is therefore an important source of information for the Commission to detect non-compliance with the DMA obligations. Given these power asymmetries and information gaps, it is a sensible choice to develop procedures for whistleblowing, and a whistleblower tool to allow stakeholders to come forward anonymously.

At first glance, extending the scope of the WBD to the DMA seems to fill this gap. However, a closer look at the design and scope of the WBD reveals shortcomings and

[27] European Commission (n 20).

[28] Marcum and Young (n 23).

[29] FM Teichmann and C Wittmann, 'Whistleblowing: Procedural and Dogmatic Problems in the Implementation of Directive (EU) 2019/1937' (2022) 30 Journal of Financial Regulation and Compliance 553.

[30] Lonati (n 12) 117–118; Wils (n 9) explains that—in competition law proceedings—information may be redacted in a file if this leads to the possible identification of a (partially) anonymous informant. See also See W Wils and A Abbott, 'Access to the File in Competition Proceedings Before the European Commission' (2019) 42 World Competition 255, updated version accessible at http://ssrn.com/author=456087.

[31] See in this regard, European Commission, 'DG Competition Informal Guidance Paper on Confidentiality Claims' (2012) Communications of the Commission 1–18.

[32] See Lonati (n 12).

[33] ibid, see also Beijer and Hoorn (n 21).

[34] J van den Boom and others, *Digital Regulation Synthesis: Comparative Analysis of the DMA, Sec. 19a and the DMCCA* (15 December 2024). Available at SSRN: https://ssrn.com/abstract=5079869 or http://dx.doi.org/10.2139/ssrn.5079869, accessed December 2024; R Podzun, 'Ch. 1 Introduction' in R Podszun (ed), *DMA article-by-Article Commentary* (Hart Nomos 2024) 1–9.

[35] Rec 7 DMA.

conceptual inconsistencies when applied in the DMA context. It remains unclear what protection is actually offered to business users that come forward, and how assurances can be made that they are protected effectively. The protection of whistleblowers cannot exist *only* in promises of anonymity: what happens if the identity of the complainant becomes known? What rights will they have? It is questionable whether the introduction of the DMA Whistleblower Tool, in the absence of clear procedural rights for third parties in DMA proceedings, is suitable to overcome these shortcomings, to fill information gaps, and to protect informants from retaliation.

Against this background, the analysis in the following section is divided into three parts. The first part assesses the background, scope, and requirements as well as some of the shortcomings of the WBD ('The scope and limits of the WBD' section). Secondly, the article takes a closer look at the protection of whistleblowers in the form of third parties under the DMA itself, including under the DMA Whistleblower Tool, and whether this reflects requirements of the WBD ('The WBD and the DMA—how has integration taken place?' section.). Section 'Shortcomings of incentives and protections for whistleblowers under the DMA' identifies some conceptual and practical issues and ambiguities related to the application of the WBD to the DMA, on the one hand, and the actual possibilities of reporting under the DMA. It finds that taking inspiration from the WBD without offering procedural rights, as granted under competition law, may create unclear expectations for potential whistleblowers and limit the effectiveness of the granted protection.

The scope and limits of the WBD

Recognizing the importance of whistleblowers to detect DMA infringements, the DMA foresees the application of the WBD to the reporting of breaches of the DMA in the Recitals 102, 103, and Article 43 DMA. This warrants a closer look at the Directive in relation to the DMA. The WBD has been introduced with specific types of whistleblowing in mind. It was introduced following high-profile cases of whistleblowers, such as those involving Edward Snowden, Julian Assange, or Chelsea Manning, that have driven global discourse on how to protect such insider informants.[36] While compliance with the DMA is mandatory, establishing non-compliance requires an investigation into the facts, and is not as easily established as clear infringements in matters of law, such as the dumping of toxic waste or financial fraud.

Legislative history and purpose of the WBD

High-profile whistleblower cases have driven a shift in perception, and ultimately prompted the debate on the adequate level of protection for whistleblowers. Before the EU introduced the WBD, the legal landscape for the protection of whistleblowers within the EU was fragmented, mostly based on initiatives from the Council of Europe and the European Court of Human Rights, and often limited to political whistleblowing.[37]

The introduction of the WBD provided minimum harmonization for the protection of employees and insiders who wished to provide information in work-related contexts.[38] With this, the Directive filled an important legislative gap, yet the implementation remained with Member States, shaped by national cultures and preferences, as well as organizational culture.[39] Against this background, Recitals 4 and 5 of the WBD lay down, as purposes of the

[36] Teichmann and Wittmann (n 29) 553–566.

[37] A Van Waeyenberge and Z Davies, 'The Whistleblower Protection Directive (2019/1937): A Satisfactory but Incomplete System' (2021) 12 European Journal of Risk Regulation 236, 236, with reference to *Guja v Moldova* Application no 14277/04 (ECtHR, 12 February 2008); V Abazi, 'The European Union Whistleblower Directive: A 'Game Changer' for Whistleblowing Protection?' (2020) 49 Industrial Law Journal 640.

[38] ibid (n 37) 643.

[39] ibid, 654.

Directive, the improvement of the protection of whistleblowers in EU Member States by establishing a minimum standard of protection in the fragmented landscape across different policy areas in the EU. Interestingly, the WBD focuses on enhancing of Union law and policies in specific areas (Article 1 WBD), describing reports and public disclosures as an 'upstream component' of such enforcement (Recital 2 of the WBD) as its main goal—rather than making worker protection or freedom of expression the primary objective of the Directive. A possible explanation for this framing of the purpose of the Directive can be found in the legal basis for the Directive, which is based on harmonization and the protection of internal market interests, in Article 114 TFEU—a similarity the WBD shares with the DMA.[40]

Material and personal scope of protection

The WBD has a broad material scope, covering many areas of Union law, as well as personal scope regarding protected individuals.

The material scope is covered in Article 2 WBD. Article 2 paragraph 1(a) WBD lists 10 policy fields to which the WBD applies, limited to the Union acts set out in the Annex to the WBD.[41] Article 51 DMA adds the DMA to Part I, section J, of the Annex to the WBD. Hence, the DMA is considered an EU act within the policy field that serves to protect privacy and personal data, as well as the security of network and information systems.[42]

Regarding the personal scope, the Directive chose a much broader scope of application than focusing only on the traditional, employee-centric conception of a whistleblower.[43] Instead, Article 4 WBD sets out a broad list of persons to whom protection should be granted, including employees, but also workers supervised by contractors or suppliers. The personal scope of application of the WBD therefore covers the typical business user of a digital platform designated as a gatekeeper under the DMA, such as an app developer developing for the Google Android operating system.

The level of protection foreseen under the WBD for persons covered by it is rather extensive. Any form of retaliation, as defined broadly in Article 5(11) WBD and further specified by a list of examples in Article 19 WBD, is prohibited.[44] Chapter VI of the WBD specifies the protective measures the WBD should take. This includes protection against retaliation (Article 21 WBD), as well as the requirement for Member States to ensure adequate penalties, *inter alia*, for hindering reporting and retaliation measures (Article 22 WBD). One particular noteworthy aspect in this context is the reversed burden of proof. Once the whistleblower demonstrates *prima facie* that the reported breach was within the scope of the WBD and that the whistleblower then suffered a detriment, 'the burden of proof should shift to the person who took the detrimental action'.[45] In the DMA context, such a system of penalties, in combination with a reversed burden of proof, may prevent direct retaliation actions, such as Apple's termination of Epic's App Store, as mentioned above.[46] However, retaliation

[40] ibid, 654.

[41] The respective policy fields are public procurement, financial services, products and markets, prevention of money-laundering and terrorist financing, product safety and compliance, transport safety, protection of the environment, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, protection of privacy and personal data, and security of network and information systems.

[42] In addition to these policy fields and specified acts, the WBD also covers breaches affecting EU financial interests pursuant to art 325 TFEU (art 2 para 1 b) WBD) as well as breaches relating to the internal market (art 2 para 1 c) WBD).

[43] Abazi (n 37) 643.

[44] art 5(11) WBD defines retaliation as any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person.

[45] Rec 93 WBD.

[46] M Acton, 'EU Probes Apple over App Store Shutdown of Epic Games' *Financial Times* (7 March 2024), online.

against business users of designated digital platforms can also be much more ambiguous, for instance, through changes to algorithms or rankings, and therefore much harder to establish, irrespective of who faces the burden of proof.[47]

Reporting channels—a three-tiered model

The core of the WBD is the requirement for Member States to ensure that three reporting channels are available to whistleblowers: internal reporting (Chapter II WBD), external reporting (Chapter III WBD), and public disclosure of relevant information (Chapter IV WBD).

Internal reporting refers to the workplace or the organization concerned by the whistleblower's disclosure. In the private sector, only companies with 50 employees or more need to set up reporting channels.[48] The rules included in Chapter II WBD impose concrete obligations on companies. It requires organizations to establish an internal or external mechanism, for example, a responsible person or department, or third-party organization,[49] for reports made by whistleblowers.[50] Procedural rules require acknowledgement of receipt of the report as well as follow-up obligations within a specific period of time.[51]

External reporting refers to the relevant authorities outside the organization concerned,[52] and may include law enforcement authorities, as well as ombudsmen or other administrative oversight bodies.[53] The reporting procedure and follow-up obligation is similar to the procedure established for internal reporting channels.[54]

Public reporting channels refer to disclosures made by the whistleblower to public channels such as the media. As the main difference from internal and external reporting channels, public disclosures require an additional threshold to be met in order for the protection of the WBD to apply, which is set out in Article 15(1) WBD.[55]

The three-tiered model of reporting channels available for whistleblowers can therefore be considered a ranked system: Internal reporting takes precedence before external reporting unless the breach of EU law cannot be addressed effectively internally, and the reporting person considers that there is a risk of retaliation. However, there is no impact on the level of protection if these requirements are not met.[56] Public disclosure can be considered subordinate within the reporting system of the WBD, as it has higher requirements in order to qualify for the protection under the WBD.

The WBD—still a long way?

The WBD has been a long time in the making, yet the law remains controversial and its efficacy unclear. The Directive was introduced on the 23rd of October 2019, and the European Parliament has called for such a regime for a decade before,[57] yet the transposition deadline

[47] In the *Google Shopping* case, it has been discussed how changes to the Panda algorithm strategically disadvantaged its competitors in comparison shopping services. See T-612/17, *Google and Alphabet v Commission*, ECLI:EU:T:2021:763, Judgment of 10 November 2021 (Google Shopping) paras 59, 282, 360ff.

[48] art 8 (3) WBD.

[49] See, eg, the KPMG Whistleblower Channel as an external mechanism for internal reporting (online).

[50] art 8 WBD.

[51] art 9 WBD.

[52] art 11 WBD.

[53] See Abazi (n 37) 650.

[54] art 11 WBD.

[55] Reports made internally or externally were made unsuccessfully previously as no appropriate action was taken, or the whistleblower has reasonable grounds to believe that the breach of Union law may 'constitute an imminent or manifest danger to the public interest' or in the case of external reporting, 'there is a risk of retaliation or there is a low prospect of the breach being effectively addressed'.

[56] art 7(2) WBD.

[57] See eg Abazi (n 37) 640.

of 17 December 2021 was only met by three EU Member States. In its report from 3 July 2024, the Commission stated that, as of the date of the report, the Commission had opened infringement proceedings against 24 Member States for failing to transpose and notify complete transposition.[58] Reliable statistics on the success of the WBD are therefore lacking from the report, given the delayed and incomplete transposition. The report identified a long list of improvements to the transposition of the WBD. In relation to the material and personal scope, conditions and measures for protection against retaliation, transposition measures were considered incomplete in many EU Member States.[59]

However, not only has its transposition, but also the WBD itself, been the subject of criticism, specifically for being inconsistent.[60] One noted inconsistency refers to ambiguity regarding the requirements and protection of anonymous reporting specifically.[61]

First, the term 'anonymity' is not coherently applied throughout the Directive, as it seems to cover both full anonymity as well as partial anonymity, as distinguished in 'The distinction between full, partial, and non-anonymity' section of this article. Recital 17 WBD refers to the 'anonymous whistleblower tool' under EU competition law to highlight policy areas where the importance of insider reporting in detecting EU law infringements has already been recognized—thus, referring to full anonymity. In Recital 30, however, the WBD applies the term 'anonymous' for partial anonymity, that is, anonymity not vis-à-vis the authority, to exclude the application of the WBD to cases in which informants are registered with a national authority as such and report in return for reward or compensation.

Secondly, while the WBD seems to value the importance of full anonymity, it leaves important aspects of anonymity at the discretion of Member States. Article 6(2) WBD, for example, states that the WBD does not affect the power of the Member States to decide whether private or public organizations, as well as authorities, are required to accept and follow up on (fully) anonymous reports of breaches. On the other hand, Recital 40 and Article 6(3) WBD envisage, without Member State discretion, that persons who anonymously reported or made anonymous public disclosures falling within the scope of the WBD should enjoy the protection against retaliation granted by the WBD if they are identified later on.

Both ambiguities in the WBD and inconsistent and incomplete transposition by EU Member States risk legal certainty, which is essential for the effectiveness of the whistleblower regime established by the WBD to reach its objective of encouraging reporting and thus strengthening effectiveness of EU law. The Commission itself stressed this point in its report on the WBD transposition: to be able to make informed decisions, the Commission highlighted that informants depend on legal certainty to be able to fully understand the extent of their rights and protections. Otherwise, they would face 'the risk of "falling between the cracks" because of the vagueness or ambiguity of the applicable rules'.[62] It is then surprising that the DMA Whistleblower Tool seems unable to grant exactly that, that is, clarity and legal certainty to business users in terms of their rights and protections, as explained below.

[58] European Commission, Report from the Commission to the European Parliament and the Council on the implementation and application of Directive (EU) 2019/1937 of the European Parliament and the Council of 23 October 2019 on the protection of persons who report breaches of Union law, 3 July 2024, 2.

[59] ibid 2ff.

[60] See eg Teichmann and Witmann (n 29) 553–566.

[61] ibid.

[62] European Commission (n 58) p 9.

The WBD and the DMA—how has integration taken place?

The DMA is often viewed as competition law-inspired, given its reliance on landmark competition law cases against Big Tech platforms.[63] However, when it comes to the role of third parties generally, and of their anonymity specifically, the DMA legislators have chosen to treat them primarily as informants without significant procedural rights. This marks a clear departure from EU competition law, where the rights and protected status of third-party informants are explicitly recognized.[64] Instead, the DMA relies only on an extension of the scope of the WBD to the DMA to incentivize whistleblowers to come forward and protect them from retaliation by gatekeepers.[65]

Against this background, the following sections analyse how this legislative choice is reflected in the set-up of the DMA, including the role of third parties and whether fully or partially anonymous reporting of DMA breaches is reflected by the provisions of the DMA and in the introduced DMA Whistleblower Tool.

The role of third parties, whistleblowers, and anonymity in the DMA

Third parties that are in a position to report on DMA breaches by gatekeepers will often be business users and thus economically dependent on—and often competing with—the gatekeeper. Therefore, these third parties will—in many cases—have a strong interest in remaining anonymous vis-à-vis the gatekeeper and in ensuring that the information they provide to the Commission receives confidential treatment.[66] In Recitals 102, 103 of the DMA, it is acknowledged that such whistleblowers can play a valuable part in enforcing the DMA obligations by bringing new information to the attention of competent authorities. Recital 102 requires that adequate arrangements are in place to enable whistleblowers to alert the competent authorities to actual or potential DMA infringements and to protect the whistleblowers from retaliation. Recital 103 of the DMA stipulates that while the transposition of the WBD is up to the Member States, transposition is not required for the applicability and protection granted under the WBD for reporting breaches of the DMA.

However, besides this legislative choice in the DMA to extend the scope of the WBD to the DMA,[67] neither the DMA nor its impact assessment materials[68] directly envisage fully anonymous reporting or complaint channels, or protection measures as required by the WBD. The necessity to protect end users or business users of gatekeepers who complain about practices violating the DMA is only briefly mentioned in the DMA in relation to a substantial obligation.[69]

First, the requirement to safeguard the right of whistleblowers to raise issues of DMA non-compliance with the relevant authorities is reflected in Recital 42 DMA, accompanying the substantive obligation under Article 5(6) DMA, which prohibits a gatekeeper from preventing business users or end users from raising non-compliance issues with authorities. The term 'whistleblowers' did not find its way into the text of Article 5(6) DMA itself despite being explicitly mentioned in Recital 42, which states that '[t]o safeguard a fair commercial

[63] A De Streel and P Larouche, 'The European Digital Markets Act: A Revolution Grounded on Traditions' (2021) 12 (7) Journal of European Competition Law & Practice 542 et seq.; Podszun and others, 'DMA Commentary' in Beck, Hart and Nomos (eds) art 34 DMA, para 19.

[64] See Art. 27(1) Council Regulation (EC) 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2003] OJ L1/1 (Regulation 1/2003) and Art. 5 and 16 Commission Regulation (EC) 773/2004 of 7 April 2004 relating to the conduct of proceedings by the Commission pursuant to Articles 81 and 82 of the EC Treaty [2004] OJ L123/18 (Reg. 773/2004).

[65] Recs 102, 103 DMA.

[66] Podszun and others (n 63) 1–9.

[67] Recs 102, 103 DMA.

[68] European Commission, *Impact Assessment of the Digital Markets Act* (2020) (online).

[69] See art 5(6) DMA and Rec 42 DMA.

environment and protect the contestability of the digital sector it is important to safeguard the right of business users and end users, including whistleblowers, to raise concerns about unfair practices by a gatekeeper'. This indicates that end users and business users can be considered whistleblowers, without further clarification on the definition of whistleblowers.

Secondly, regarding the confidentiality of the identity of informants, the procedural scope of protection in DMA procedures remains limited. Article 27 DMA clarifies that third parties can inform the Commission or the national authorities about practices of a gatekeeper that fall within the scope of the DMA. The DMA Implementing Regulation[70] offers some protection for these third parties, as they can claim their information to be treated confidentially if it qualifies as business secrets. Confidential information can include the identity of the third party if it is legitimately concerned that the gatekeeper will engage in commercial retaliation if it becomes aware of the third party's identity.[71] Article 7(7) of the DMA Implementation Regulation therefore stipulates that third parties submitting comments have the right to request redaction of any identifying information before the comments are shared. In terms of procedural clarity, Article 27 DMA does not, however, offer much legal certainty for third parties that come forward. Unlike the WBD, which establishes follow-up rules for authorities that receive reports, Article 27 paragraph 2 DMA grants full discretion to the Commission and national authorities as regards following up on the information received and the appropriate measures to be taken.

In short, the DMA itself remains very shallow in relation to the procedure third parties should follow if they want to report on DMA breaches. While the law acknowledges the role of third parties as informants, it does not clarify how they should be protected from retaliation if their identity is disclosed, nor how authorities shall treat the information received. The introduction of the DMA Whistleblower Tool, discussed hereunder, addresses some of these shortcomings in order to encourage third parties to come forward.

Protection of anonymity through the DMA Whistleblower Tool

The DMA Whistleblower Tool is offered in the form of an online portal. Through this portal, the Commission invites contributions from employees, ex-employees, and third parties, specifically mentioning reports, email exchanges, data metrics, internal research, and decisions.[72] To submit anonymous or attributed information, informants are guided through a report form that requests a description of facts and the relationship between the informant and the gatekeeper, and enables third parties to upload files. In this form, informants can choose whether they want to stay anonymous or provide contact details. Anonymization will be ensured by a secure inbox, encryption, and other special security functions.[73] The Whistleblower Tool also enables communications between the informant and the Commission via a secure inbox within the tool. According to information available on the Commission's website, this secure inbox will serve as the medium to receive feedback, follow-up questions, and feedback on the progress of the report made from the Commission, and it will be available either in anonymous or attributable mode.[74] However, the Commission does not seem to tie itself to strict follow-up deadlines or to an obligation to respond to reports, as required by Article 11 WBD.

[70] Commission Implementing Regulation (EU) 2023/814 of 14 April 2023 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/1925 of the European Parliament and of the Council.

[71] Podszun and others (n 63) para 23.

[72] Commission, *DMA Whistleblower Tool* (online).

[73] ibid—FAQ (online).

[74] See the Whistleblower Tool itself here, online.

Overall, the design of the DMA Whistleblower Tool resembles the design of the competition law whistleblower Tool.[75] Here, individuals and companies are invited to inform the Commission about any breach of EU competition rules, including price coordination, bid rigging, unfair exclusions of rivals, or gun jumping in merger cases. Informants also have the option to either reveal their identity to the Commission or stay anonymous and communicate through an intermediary's encryption tool that allows for two-way communication. The introduction of the competition law whistleblower Tool was reportedly a response to a 58% drop in leniency applications between 2015 and 2021.[76] The Commission had heavily relied on leniency applications, which are said to have helped uncover two-thirds of all detected cartels.[77]

Hence, the Commission may have built on its experiences with the competition law Whistleblower Tool when setting up the DMA Whistleblower Tool. Approximately 100 reports per year were sent through the competition law tool.[78] Nevertheless, absent any statistics on how successful reports through the (anonymous) competition law Whistleblower Tool have proven to be for law enforcement, it will be difficult to make any predictions as to whether the DMA Whistleblower Tool will have a significant impact on detecting DMA violations by gatekeepers. It is, however, unlikely to reach a similar success quote as leniency applications. Unlike leniency applicants, who are incentivized by a reduction of fines if they come forward to inform about a cartel, neither the DMA nor the competition law Whistleblower Tool foresees a similar reward for coming forward other than the prospect of law enforcement.

Shortcomings of incentives and protections for whistleblowers under the DMA

Looking at the purpose of the WBD—strengthening the enforcement of EU law by encouraging whistleblowers to come forward and providing a high level of protection from retaliation—the application of the WBD to the DMA does not seem inconsistent at first glance, given the power asymmetries between gatekeepers and business users.[79]

However, absent further procedural and protective rights under the DMA for third parties to participate more actively in DMA enforcement, the DMA's reliance on the WBD and the introduction of the DMA Whistleblower Tool to create a forum for third parties and to encourage them to come forward and report (anonymously) on DMA breaches reveals several shortcomings. These may cause uncertainty for potential whistleblowers, which may impact their incentives to come forward. The shortcomings identified relate to conceptual discrepancies between the WBD and the DMA, which may limit the applicability of protections offered in the WBD ('Conceptual gaps between the WBD and the DMA' section) and to the gap between third-party participation in competition law proceedings versus DMA proceedings. The latter shows that the introduction of the DMA Whistleblower Tool alone may fall short of delivering equal success as the EU competition law regime ('Why the DMA Whistleblower Tool is unlikely to deliver like its competition law twin' section).

Conceptual gaps between the WBD and the DMA

The identified conceptual gaps between the WBD on the one hand and the DMA on the other relate to institutional, substantial, as well as procedural discrepancies between the two legal instruments.

[75] For general background information by the European Commission, see online.

[76] OECD, 'The Future of Effective Leniency Programmes: Advancing Detection and Deterrence of Cartels' *OECD Competition Policy Roundtable Background Note* (2023).

[77] Jones Day, *European Commission Launches Competition Law Anonymous Whistleblower Tool, Jones Day Commentary* (2017) (online).

[78] Insight EU monitoring, *Competition: EU Commission Extends Scope of Anonymous Whistleblower Tool* (2023) (online).

[79] Podszun, *DMA Commentary*, art 5(6) DMA, para 125.

First, from an institutional perspective, the DMA, with the Commission as sole enforcer, does not envisage decentralization of enforcement and the collection of information.[80] However, the WBD is a Directive that is addressed to Member States to establish appropriate external and internal information channels for whistleblowers and to ensure adequate protection from retaliation, and leaves various aspects to the discretion of Member States, for example, whether fully anonymous reporting should be enabled. This divergence of competencies is also not remedied by Recital 103 DMA, which states that the 'adoption of national transposition measures is not a condition for the applicability of that Directive to the reporting of breaches of this Regulation and to the protection of reporting persons from the date of application of this Regulation'. Without transposition measures by Member States to ensure protection for whistleblowers, and given the absence of a protective mechanism under the DMA itself, the scope of protection and enforcement against retaliation measures remains vague and does not offer sufficient legal certainty for potential informants.

The second discrepancy identified relates to the material scope of protection envisaged by the WBD, which seems to differ to some extent from the one addressed by the DMA. The WBD typically relates to the relationship between an employee and their employer, even though the personal scope of the WBD is rather broad. Recital 1 WBD refers, for example, to any 'persons who work for a public or private organization or are in contact with such an organization in the context of their work-related activities'. Following this broad reading, not only employees of an organization potentially in breach of EU law can be whistleblowers for the purpose of the Directive, but also persons who are in contact with such an organization, such as business users of a gatekeeper designated under the DMA.[81] This is supported by the assumption that business users generally have a similarly asymmetrical power dynamic with their gatekeeper, characterized by dependencies, as employees do with their employer. There are, however, parts of the WBD that do not match the setup of the DMA well, as they presuppose reports made by employees rather than business users or competitors. The identified types of retaliation and the scope of the behaviour that can be penalized, for example, do not clearly correspond to the DMA. Specifically, Article 19 WBD lists examples of potential retaliation measures, which apply in their majority to employer–employee relationships rather than business or competitor relationships, such as, for example, disciplinary measures or withholding of promotions. In addition, from a practical perspective, the WBD envisions types of retaliation that are explicitly targeting the informant. As discussed *supra*, retaliation can also happen more generally or indirectly by changes to the business model, or tweaks to the terms and conditions for access. Consequently, potential retaliation under the DMA may require a broader approach to standards for assessment of retaliation measures, covering a wider range of behaviours that directly or indirectly harm informants, including rules that apply to business users generally. Google's implementation of its compliance mechanisms following the *Google Shopping* case, as well as the mandatory compliance with Article 6(5) DMA, have shown how complex interactions between a gatekeeper and its business users leave space for varying forms of retaliation. In the *Google Shopping* case, Google's chosen compliance mechanisms made competing comparison shopping suppliers (CSS), the complainants in the case, worse off.[82] Google's measures to comply with Article 6(5) DMA have

[80] See arts 20 DMAff.

[81] F Kain, 'Whistleblowing and Labour Law: The Whistleblower Directive -Development, Content and Obstacles' (2020) 2 Italian Labour Law E-Journal, supports such a reading, stating that the 'Whistleblower Directive also encompasses other people as long as they are vulnerable in the context of their work-related activities.'

[82] Google designed the auction of listings on the Google Search page in a manner that intensified competition between third-party CSS suppliers themselves, between CSS suppliers and advertisers, and by raising the price for leads through the Shopping Box. The initial complainants have sounded the alarm about these compliance mechanisms on many different occasions, see F Scott Morton and J Van den Boom, 'Are Competition Authorities Equipped to Combat Entrenched Digital

similar effects, intensifying competition between direct providers of search results and vertical search service providers such as CSSs, reducing the attractiveness of the services offered by the latter for consumers. With its changes, Google directly and indirectly punishes the group of users that has been most vocal about the need for regulation.[83] Retaliation against a sector of business users as a whole disguises whether this is retaliation against one single business user, a group of users, or just a change in policy. Thus, it will be hard to prove that changes to the business model of the gatekeeper are part of a retaliatory effort.

Thirdly, the procedures for reporting DMA breaches seem largely misaligned between the DMA and the reporting requirements established under the DMA. The DMA already includes provisions such as Article 5(6) DMA and Article 27 DMA, which foresee a scenario where gatekeepers' users raise issues of non-compliance with authorities. The DMA even requires gatekeepers to set up an alternative dispute settlement mechanism for solving disputes around access for business users to its software application stores, online search engines, and online social networking services, in Article 6(11) DMA. These rules create similar procedures to those related to internal reporting requirements. Nevertheless, the DMA legislators omitted the opportunity to require gatekeepers to establish internal reporting channels aligned with the requirements of Article 7 WBD. This seems somewhat inconsistent, as the WBD gives precedence to internal reporting in Article 7(2) WBD unless the 'use of internal channels cannot reasonably be expected to function properly', that is there is a valid risk of retaliation measures or that competent authorities would be better placed to take effective action to address the breach.[84] However, as the DMA envisages internal dispute mechanisms in Article 6(11) DMA, it remains unclear why a requirement to set up an internal reporting channel with the protections and requirements of the WBD was not established under the DMA, despite the clear intention to extend the scope of the WBD to the DMA in Recital 103 DMA.

Against this background, the general extension of the WBD to apply to reporting of DMA breaches may not reflect the nature and content of the DMA accurately. Therefore, the idea reflected in Recital 103 DMA, that the WBD should impose a general duty to 'be ensured that adequate arrangements are in place to enable whistleblowers to alert the competent authorities to actual or potential infringements of [the DMA] and to protect the whistleblowers from retaliation', seems to pass over too quickly the problems that would arise in translating the personal scope, general principles, remedies, and sanctions provided for in the WBD currently.

Why the DMA Whistleblower Tool is unlikely to deliver like its competition law twin

Prima facie, the DMA appears to be fertile ground for third-party input on the gatekeepers' compliance efforts. The law is designed as an *ex ante* regulation with a set of clear, self-executing obligations. Unlike in competition law cases, where an infringement of competition law must be established by the authority, establishing non-compliance under the DMA appears to be—arguably—less complex from a third-party perspective. This is further facilitated by the transparency obligations on gatekeepers to document and publish their compliance efforts in annual compliance reports.[85]

Monopolies? -Lessons from the US and EU Antitrust Cases against Google' Northern Illinois Journal of Law, Technology and Policy (2025), preprint available on SSRN, 22–24.

[83] EU Travel Tech, 'Google's Deceptive DMA (non-)Compliance Tactics' (*EU Travel Tech Blog*, 13 December 2024) (online).

[84] Rec 62 WBD.

[85] art 11 DMA.

However, relying solely on the DMA Whistleblower Tool may not provide the expected incentive for third parties, particularly business users, as it does not provide the right venue and rewards similar to those for reporting competition law breaches.

The first shortcoming relates to the ambiguity of the DMA Whistleblower Tool, which seems to be a black box for potential whistleblowers in terms of clarity of their impact, rights, and protections. Third parties who submit information to the Commission through the tool—anonymously or not—do not have the right to be involved in possible future proceedings. Moreover, the Commission has a wide discretion as to which instances of non-compliance it will investigate. Therefore, from the whistleblower's perspective, it is unclear what level of information provided will trigger an investigation. Finally, the Commission has not issued clear procedural guidelines on how to protect the identity of complainants.[86] This means that there are too many unanswered questions, that is risks, for whistleblowers: they do not know how detailed the information they need to provide should be, how their identity will be protected, and what will happen if their identity is revealed. There are also no rewards for coming forward: after providing the initial information, it is not clear whether and how the business user will be consulted in the investigation. There is also no certainty that the business user will be able to influence the compliance strategy following the investigation.

This is closely related to the second shortcoming, which is that third parties who wish to come forward to report DMA breaches do not have the same opportunities and rewards as whistleblowers on competition law breaches. Under competition law, third parties not only have the possibility to report through the Competition Law Whistleblower Tool, but they can also formally join proceedings or make use of the leniency programme. In addition, the decentralized enforcement system of EU competition law between the Commission and the national competition authorities provides further reporting possibilities.

In competition law proceedings, including the prohibitions set out in Articles 101 and 102 TFEU, third parties are considered an important source of information and are invited to participate in antitrust proceedings. In the case of Article 101 TFEU in particular, leniency can be considered the most important tool in the detection of cartels. Getting an insider to come forward is the most direct way to gain insight into the functioning of the cartel and the associated competitive harms. Therefore, the scenario that the Commission had in mind when introducing the Competition Law Whistleblower Tool was primarily cartel cases under Article 101 TFEU. While leniency applications reportedly contributed to two-thirds of cartel investigations,[87] the success rate of information provided through the Competition Law Whistleblower Tool is not publicly known but is most likely much lower, as the incentive to report under the leniency programme is clear compared to reporting through the tool: leniency applicants face no or reduced fines as a reward for reporting.[88]

In addition to the leniency programme, the Competition Law Whistleblower tool is complemented by another way for third parties to inform the Commission about competition law breaches. Under EU competition law, complainants can become 'closely associated' with a case. A party that is closely associated with the case is granted procedural standing. This allows the complainant to protect its own interests in the procedure by providing opinions, insights, and information. Complainants who wish to keep their identity confidential have the same procedural rights as identified complainants. Therefore, the scope of protection of a complainant's identity vis-à-vis the investigated undertaking goes well beyond the initial

[86] On its website, the European Commission only provides limited, non-binding information regarding the protection, and further procedure for whistleblowers, see online.

[87] ibid.

[88] See Commission Notice on Immunity from fines and reduction of fines in cartel cases, C-289/17 (2006).

information, and the importance of confidential complaint channels is well documented and established in EU competition case law.[89] The Commission has also ensured that the possibility of remaining unidentifiable to other parties is embedded in its procedures and forms.[90] The partial anonymity of the complainant is protected throughout the procedure, and information exchanged with national competition authorities and courts is also anonymized.[91]

In addition to these established procedures to protect the identity of third parties, the enforcement of EU competition law relies on a decentralized enforcement system within the European Competition Network (ECN) based on Articles 4 and 5 Regulation (EC) 1/2003.[92] Thus, in addition to the channels established by the Commission, be it in the form of the Competition Law Whistleblower Tool, leniency or formalized procedural participation, third parties can also rely on the national competition authorities in their respective Member States as a first point of contact for reporting potential competition law breaches. This is not the case in the DMA, where the Commission acts as the sole enforcer.[93]

These barriers to reporting are particularly problematic for the DMA, where there are virtually no other third-party participation rights. If the DMA Whistleblower Tool cannot provide business users with the certainty that they will be protected, they are unlikely to take the risks associated with coming forward about potential non-compliance in one or more areas. This is particularly true for smaller, more vulnerable business users, and is likely to affect the effective enforcement of compliance with the DMA in the absence of essential input from industry insiders. It therefore remains to be seen how effective the DMA Whistleblower Tool will be in encouraging whistleblowers to come forward without any further rights and opportunities to shape potential subsequent investigations and proceedings.

4. THE WAY FORWARD—THE BALANCING ACT OF WHISTLEBLOWER PROTECTION AND ENFORCEABILITY IN THE DMA

It seems that (incentivizing) third-party participation was neither a priority for the legislator nor the Commission in the genesis of the DMA. As stated above, the DMA does not contain any further participation rights for third parties beyond making statements and comments upon invitation by the Commission. In the original proposal of the DMA text by the Commission, protection of whistleblowers was not even envisaged.[94] The latest example of de-prioritizing the role of third parties in DMA proceedings could be seen in the announcement of the DMA Whistleblower Tool weeks after the first non-compliance investigations had already been initiated by the Commission.[95] While the opening of a non-compliance investigation has been lauded by interested stakeholders, the swift initiation of non-compliance proceedings by the Commission only weeks after the obligations imposed in the

[89] Case C-94/00 *Roquette Frères*, ECLI:EU:C:2002:603, Judgment of 22 October 2002, para 64; Case C-310/93 P, *BPB Industries plc and British Gypsum Ltd v Commission*, ECLI:EU:C:1995:101, Judgment of the Court (Sixth Chamber) of 6 April 1995, para 26; Case C-310/93 P, *BPB Industries plc and British Gypsum Ltd v Commission, Summary*; Case T-221/95 *Endemol v Commission [1999] ECR II-1299*, para 69, and Case T-5/02 *TetraLaval v. Commission* [2002] ECR II-4381, para 98ff).

[90] Procedural rules for competition law can be found in Regulation 773/2004; Regulation 1/2003.

[91] See Wils (n 9).

[92] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in arts 81 and 82 of the Treaty.

[93] See art 20 DMAff.

[94] See European Commission, Proposal for a Regulation of the European Parliament and Council on contestable and fair markets in the digital sector, COM/2020/842 final (2020) (proposal for the Digital Markets Act).

[95] The first investigations into non-compliance were announced on the 25th of March 2024, the Whistleblower Tool was not introduced until 30 April 2024, see European Commission, Commission opens non-compliance investigations against Alphabet, Apple, and Meta under the Digital Markets Act, Press Release of 25 March 2024; European Commission, Commission launches Whistleblower Tools for Digital Services Act and Digital Markets Act, Press Release of 30 April 2024.

DMA became applicable also shows that the DMA is far less self-executing than anticipated in the legislative process.[96] Consequently, the Commission will have to rely on inside information by market participants, be it business users, competitors, end users, or gatekeeper employees, to enforce the law. Perhaps more than initially expected.[97]

The introduction of the DMA Whistleblower Tool can be considered as a first step for the Commission in establishing clear information channels to overcome information asymmetries and to benefit from inside information provided by industry participants. However, there are several alternative proposals worth considering to incentive further contributions from third parties while protecting them from retaliation from gatekeepers, even within the limited procedural participation rights granted to third parties under the DMA. Each of the proposals set out in the following sections takes into account the benefits and drawbacks of the different levels of anonymity of informing third parties as established in the 'Benefits and drawbacks of different levels of anonymity' section.

Increasing procedural transparency

As the Commission stressed in its report on the transposition of the WBD, legal certainty is key to encouraging informants to report on breaches of EU law as they must be put in a position to fully understand the extent of their rights and protections.[98] This is why procedural clarity and transparency are essential also for potential whistleblowers for DMA breaches.

Therefore, a first proposal, with low intervention intensity in terms of implementing efforts, to encourage more informants to come forward while not risking swift enforcement efforts and sacrificing large amounts of staff resources, could be to introduce clearer and more transparent information and rules on how the Commission will follow-up within the DMA Whistleblower Tool.

Currently, the Commission only provides limited information regarding the use of the DMA Whistleblower Tool on its website. While it explains what types of complaints it allows, and how they can be lodged, it falls short in explaining what level of information is required to trigger the Commission's interest. Moreover, there is no explanation of what measures are taken to protect their identity or communicate with them (if they lodge the complaint under partial anonymity). In order for parties to come forward, they must be afforded a certain sense of security or trust. Hence, more detailed guidance and commitment by the Commission are warranted.

For this purpose, the follow-up requirements under the WBD can serve as the departing point. For external reporting channels, Article 13 WBD, for example, requires publication on the website of 'the procedures applicable to the reporting of breaches, including the manner in which the competent authority may request the reporting person to clarify the information reported or to provide additional information, the timeframe for providing feedback and the type and content of such feedback'. Information on follow-ups and timelines could be even further built-out to include standards that determine when the Commission would be required to follow-up and inform the whistleblower on a regular basis and when the Commission can dismiss information, in order to put potential whistleblowers in a position to assess whether they have sufficient information to trigger investigations. As the DMA Whistleblower Tool, unlike leniency regimes, does not foresee a reward for coming forward,

[96] European Commission ibid.

[97] The European Commission counts on input by third parties as part of its strategy, as emphasized in European Commission, Designated gatekeepers must now comply with all obligations under the Digital Markets Act, Announcement of 7 March 2024: 'Gatekeepers started testing measures to comply with the DMA ahead of the deadline, triggering feedback from third parties', online.

[98] European Commission (n 58) 9.

this is essential: the only incentive for third parties to report on DMA breaches is the benefits they are hoping to receive from law enforcement against the gatekeeper.

In addition, more information on the protection of the identity of the informant is currently lacking from the DMA Whistleblower Tool in cases where informants opt for partial anonymity, that is disclose their identity to the authority but seek protection of their identity vis-à-vis the gatekeeper. Here, the protections offered under the DMA Implementing Regulation, which require the authority to treat information that can lead to the identification of the third-party confidentially (see above), should be transferred to the DMA Whistleblower Tool in a way that provides third parties with full visibility of the scope of protection.

These changes will benefit third parties regardless of the level of anonymity chosen. For potential whistleblowers, more information helps make an informed decision about how to come forward. They can better assess whether their information will be followed up on if they lodge it fully anonymously, and may incentivize them to submit information under partial anonymity or disclose their identity if this produces further benefits. If they opt for partial anonymity, it also sheds light on how their identity will be protected and who will gain access to their identity. This may help to create trust in the process and eventually encourage third parties to come forward and make use of the reporting channel offered through the DMA Whistleblower Tool.

A greater role for national competition authorities

A second proposal to improve options for third parties to come forward and report on DMA breaches relates to robust and enhanced coordination within the ECN on information received by whistleblowers. Following the spirit of the WBD, which is directed at Member States, it should be ensured that all national competent authorities have whistleblower tools for reports on DMA breaches in place, and provide transparent and easily accessible reporting channels to informants on DMA breaches.

There are multiple potential benefits to having a decentralized approach. First, business users will likely find it easier to find the procedures implemented by national competition authorities and to contact them. In some cases, third parties may already have established relationships with national competition authorities, making it easier to come forward. National competition authorities can serve as a first point of contact and information, either helping the informant to develop their complaint, processing their complaint, or referring them to the European Commission directly. This is related to a second benefit. As the national competition authority acts as a first point of contact, it is able to weed out low-quality signals and reduce the administrative burdens of the Commission.[99] It can also process or investigate the information in the first instance and inform the Commission of the outcome of its investigation. In the case of the latter, the identity of the whistleblower (if disclosed confidentially) will remain solely with the national competition authority for longer.

Including national competition authorities in the processing of information by Whistleblowers would not only better reflect the decentralized nature of the WBD as the underlying legal ground for the DMA Whistleblower Tool, but it would also produce practical benefits. Relying on national competition authorities to serve as a first point of contact for partially or fully anonymous whistleblowers is a clear route to activate national competition authorities and to involve them in the DMA.[100] It would also allow the national competition

[99] Cedric Argenton and others, 'Can Abuse of a Dominant Position be Tackled More Effectively?' (2023) *Report for the Ministry of Economic Affairs & Climate* 68–74: most of the signals received by competition authorities—at least the Dutch competition authorities—are not worth investigating.

[100] See J van den Boom, F Bostoen and G Monti, 'The Netherlands: DMA Enforcement Paradise?' in Gabriella Muscolo and Alessandro Massolo (eds), *The DMA and More—Future Application and Margin of Manoeuvre for National Jurisdictions* (Concurrences 2025).

authority to develop mechanisms to protect the whistleblowers that are well suited to the national context, based on transposition measures of the WBD into national law. Limiting the role of national competition authorities to the first point of contact for third parties also does not constitute a systemic inconsistency in light of the DMA's centralized approach with the Commission as sole enforcer: Article 27 DMA foresees that third parties can raise complaints with national authorities, while Articles 37 and 38 DMA envisage close cooperation between national (competition) authorities and the Commission with regard to enforcement actions related to the DMA.[101]

Different effects on the incentives of the three categories of anonymity of informing third parties can be identified in relation to the proposal to strengthen the role of national competition authorities for the purpose of reporting breaches of the DMA. For third parties who prefer to disclose their identity to the authority, national competition authorities can more easily establish a basis of trust, consult on the prospects of the case and may even conduct an initial investigation into the behaviour. On the other hand, third parties who choose not to reveal their identity to the gatekeeper may be hesitant to share their identity with both the national competition authority and the Commission, as sharing one's identity with more institutions may increase the risk of being identified.[102] Nevertheless, the benefits of a de-centralized reporting system and its consistency with the spirit of the WBD and the well-established cooperation of national competition authorities within the ECN seem to outweigh such limited risks of exposure.

Requiring internal reporting channels

As mentioned above, the WBD requires the set-up of internal reporting channels for public institutions as well as for larger private undertakings, a requirement which the DMA could mirror. Systematically, this proposal would be consistent with the legislative choice of the DMA to expand the scope of the WBD to cover the DMA, as well as with the nature of the DMA, which is intended to be self-executing.

In this context, the provision of Article 6(11) DMA and its requirement for gatekeepers to set up internal alternative dispute mechanisms show that the DMA already establishes rules for how conflicts arising between business users and gatekeepers outside of the Commission's investigations should be dealt with. Thus, the possibility of internally handling reporting on non-compliance by users and the obligation to set up respective mechanisms has been foreseen under the DMA.

The requirement for gatekeepers to have alternative dispute mechanisms in place could be built out further to mirror the requirements for internal reporting channels under the WBD and to be the first point of contact for business users for any potential breaches of the DMA.[103] Obviously, gatekeepers must comply with the requirements set out in the WBD for internal reporting channels, including the confidential treatment of the identity of the reporter and protection against retaliation. For this purpose, transparency through regulatory oversight or involvement of external operators of the internal reporting channel should be considered to ensure that gatekeepers do not engage in unlawful activities to cover up DMA breaches, and are not able to identify and take retaliation measures against the reporting third party.[104] Gatekeepers could also be required to share the complaints or to send regular

[101] J Van den Boom, 'What does the Digital Markets Act Harmonize? – Exploring Interactions between the DMA and National Competition Laws' (2023) 19 (1) European Competition Journal 83.

[102] Van der Sloot and others (n 18) 1.

[103] See art 7 WBDff.

[104] Consulting firms and other third-party service providers are offering whistleblower reporting solutions, see eg, PwC's Whistleblower and Ethics Reporting Channel (online), see for an offering involving an external whistleblowing ombudsman, online.

reports on the nature of complaints they have received through the internal reporting channel with the Commission. Such a requirement could be easily reconciled with the spirit of the DMA, which requires detailed annual compliance reports from the gatekeepers on how they effectively comply with the obligations in Articles 5–7 DMA.[105] Where it does not seem sensible to enter into direct dialogue to negotiate the terms and conditions for access to the platform for specific business users because business users fear reprisals due to a conflict of interest held by the gatekeeper, the business user should still be able to report anonymously and even to skip this step and report to the public authority directly.

Requiring gatekeepers to establish robust internal reporting would also have the benefit of saving the Commission's resources for cases in which gatekeepers decide to settle DMA compliance issues internally. In terms of implementing this proposal, a change to the law of the DMA would likely be required to ensure consistent implementation across Member States. The DMA remains open to legislative changes where warranted through its review clause in Article 53 DMA. However, in order to encourage third parties who wish to stay anonymous vis-à-vis the gatekeeper to come forward and report on DMA breaches as well as to ensure overall effectiveness, such internal reporting channels must be designed in a way that they are trustworthy. Regardless of the level of anonymity that reporting third parties choose to have, internal reporting channels on DMA breaches would only be successful if they exert sufficient pressure on the gatekeeper to change its behaviour.

Introducing greater third-party rights

The most far-reaching adjustment to the whistleblower procedure would be to grant third parties an increased number of rights, equating the position of third parties closer to those granted in competition law proceedings.

The rights granted to third parties under competition law proceedings include access to the file, the right to be heard, and the right to appeal decisions by the Commission related to the investigation.[106] The situation in which third parties find themselves in the DMA is closer to competition law than it is to protection from retaliation by employers as originally foreseen in the WBD. It is mostly not individuals suffering from DMA breaches by gatekeepers but undertakings doing business with or competing with the gatekeeper. Generally speaking, such third parties are better equipped and more willing to take a more active role in proceedings against gatekeepers.

Increasing third-party rights therefore creates a reward-like situation for identifiable and partially anonymous informants, as they can formally establish their position in the proceedings. This may also move otherwise fully anonymous informants to come forward to disclose their identity, at least to the regulatory authority.

There are, however, downsides to granting third parties such a formal status of being closely associated, as the administrative burdens on the regulatory authority increase (taking statements, disclosing non-confidential versions of the file, and, in case of partial anonymity, protecting the third party's identity throughout the proceedings). One of the drivers behind the introduction of the DMA was to accelerate regulation of digital platform markets. Competition law proceedings against gatekeepers in landmark cases such as Google Shopping have taken several years until a Commission decision was taken plus judicial review.[107] Keeping procedures streamlined and ensuring swift enforcement has

[105] See art 11 DMA and European Commission, Article 11 DMA—Compliance Report Template Form (online).
[106] Wils (n 9).
[107] See Scott Morton and Van den Boom (forthcoming 82) 37.

therefore been one of the major objectives of designing the procedural provisions of the DMA.[108]

5. CONCLUSIONS

The *David v Goliath* effect of Big Tech platforms designated as gatekeepers under the DMA versus their business users creates dependencies that deter business users from coming forward and claiming their rights under the DMA. At the same time, the success of leniency applications for cartel detection, for example, shows how important inside information is for law enforcement by the Commission.

Not disclosing their identity to the gatekeeper therefore plays an important role for DMA business users that seek to report on DMA breaches. However, each of the three degrees of anonymity (full anonymity, partial anonymity, non-anonymity) established in this article for informants that come forward to inform relevant authorities about wrongdoings of specific undertakings has different benefits and drawbacks. Thus, regulators need to carefully consider how to encourage whistleblowers to come forward by properly securing their protection against retaliation measures, without significantly increasing administrative burdens and violating due process. At the same time, third parties can only make an informed choice about coming forward and the level of anonymity that they maintain if the conditions and terms for engaging with the regulator are clearly defined. Against this background, the introduction of the DMA Whistleblower Tool can be considered an important first step to incentiveze third parties that depend on non-disclosure of their identity vis-à-vis the gatekeeper to come forward and alert the Commission of DMA breaches by gatekeepers.

However, the article has identified a number of issues in relation to the role of third parties as informants on DMA breaches, their protection, and incentives to come forward as established under the DMA. First, the reliance on the WBD for protection of whistleblowers as envisaged under Recital 102 and 103 DMA reveals several conceptual discrepancies between the two legal instruments. In particular, the specific requirements of the WBD for reporting by whistleblowers are not reflected in the DMA, which creates a gap absent specific transposition by the EU Member States. The introduction of the DMA Whistleblower Tool, while creating the first forum for third parties to report to the Commission anonymously on potential breaches of the DMA, seems unlikely to be successful alone, absent complementary measures to incentivize third parties to come forward. There is a lack of clarity as to what protection is actually offered to business users through the integration of the WBD, and it is unclear whether responsibility for this protection lies with the Commission or the Member States (who do not co-enforce the DMA). Besides this risk of downsides to coming forward, the potential upsides are limited. There is no guarantee that the Commission will follow up on signals by third parties, and even if the Commission does so, the whistleblower is not granted any procedural rights to protect their interests. The position of informants is very different from what it would be if they came forward as complainants in competition law proceedings, making it unclear what DMA whistleblowers can expect.

To close information gaps, the article suggests a number of improvements and complementary measures to improve the position of third parties to come forward and provide information necessary for the Commission to effectively enforce the DMA. These consist of offering more procedural clarity about the process of whistleblowing, greater use of the capacities of the national competition authorities in facilitating whistleblowing, aligning the

[108] J Van den Boom and R Podszun, 'Procedures in the DMA: Non-compliance Navigation—Exploring the European Commission's Space for Discretion and Informality in Procedure and Decision-making in the Digital Markets Act' (2025) European Competition Journal 1–30; R Podszun (n 34) 1–9.

DMA Whistleblower Tool and WBD better by building out the role of internal reporting channels, and considering more procedural participation rights for third parties in DMA proceedings. These proposal aim to further incentivizing third parties to inform on non-compliance of gatekeepers by taking into account their necessity to not reveal their identity to the gatekeeper.

The necessity of balancing power asymmetries between Big Tech platform businesses and their users is not limited to substantive obligations for these gatekeepers to ensure contestable and fair markets under the DMA. Balancing power asymmetries must also be considered when designing the accompanying procedures for DMA enforcement. Otherwise, enforcers risk not only to oversee non-compliance practices by gatekeepers, but also risk regulatory capture if they are only dealing with gatekeepers or market participants that can afford to act against gatekeepers in the open.

ACKNOWLEDGEMENTS

We would like to thank Prof. Rupprecht Podszun, Dr Filippo Lancieri, and the anonymous reviewers and editors at the Journal of Antitrust Enforcement for their feedback in developing this research.

FUNDING

This research has been conducted for the project 'Shaping Competition in the Digital Age' (SCiDA). This project is publicly funded by the Deutsche Forschüngsgemeinschaft (DFG) and the UK Arts & Humanities Research Council (AHRC). Project number 528025333.

Conflicts of interest: None declared.

Journal of Antitrust Enforcement, 2025, 00, 1–23
https://doi.org/10.1093/jaenfo/jnaf017
Article