Holistic AI comments on the template relating to the audited description of consumer profiling techniques pursuant to Article 15 of Regulation (EU) 2022/1925 (Digital Markets Act)

15 September 2023

European Commission
Brussels
Belgium

RE: Feedback on the European Commission's template relating to the audited description of consumer profiling techniques pursuant to Article 15 of Regulation (EU) 2022/1925 (Digital Markets Act)

Dear Sir/Madam,

Thank you for the opportunity to provide our considerations on this important matter.

1. About Holistic AI

Holistic AI is an AI Governance, Risk and Compliance platform with a mission to empower enterprises to adopt and scale AI with confidence. We are a multidisciplinary team of AI and machine learning engineers, data scientists, ethicists, business psychologists, and legal and policy experts.

We have deep practical experience in auditing AI systems, having assured over 100 enterprise AI projects covering more than 20,000 different algorithms. Our clients and partners include Fortune 500 corporations, SMEs, governments, and regulators. We work with several companies to conduct independent AI Audits and offer proprietary software as a service platform for AI Governance, Risk Management, and Regulatory Compliance. Considering that AI algorithms and models are frequently used in consumer profiling, we believe that Holistic AI not only has an interest in the enforcement of DMA but can also contribute thereto.

2. Considerations

We welcome the European Commission's consultation on the template relating to the reporting on consumer profiling techniques and audit of such reports that designated gatekeepers will have to submit annually, under Article 15 of the Digital Markets Act. Auditing algorithms of any kind is a multi-faceted conduct, during which both enterprises and auditors may face uncertainties as well as complexities stemming from the current or potential divergence between prescribed regulatory provisions and actual dynamic industry practice. We appreciate the Commission's intent of providing a guideline, as well as clarity to the audit of consumer profiling techniques and would like to take this opportunity to share our views on the issue.

Before advancing further, we would like to note that we are aware that the Template is for the audit description only and does not contain information as to the audit procedure or methodology. However, as the procedure and methodology of the audit are inextricably intertwined with the description, and as Article 15 empowers the Commission to implement acts to develop the methodology and procedure of the audit, we would like to take a step further and share our views as well as proposals thereon.

2a. Title of Section 1 and Section 3

First, we would like to draw attention to the title of Section 1, which reads "General information on profiling description", whereas the questions thereunder are addressed not to describe the profiling but to, as stated in the Introduction of the Template, identify the gatekeeper as well as actors involved with the drafting of the report.

Similarly, Section 3 is entitled "General information on audit", while the questions thereunder are concerning not the audit but the auditors. We believe that converging the title and the questions may increase the legal certainty and, hence, facilitate the procedure for all stakeholders.

2b. Qualifications and independence of the auditors/auditing organisations

We appreciate the transparency on the auditors'/auditing organisations' identity and affiliations. On the other hand, we believe that it would be beneficial to both audited Gatekeepers and auditors/auditing organisations if the Commission provides guidance on the qualifications and appointment of auditors, as well as the evaluation criteria of the independence of the auditors/auditing organisations.

2c. Methodology and procedure of the audit

On a similar note, while the request for information aimed at providing transparency with respect to consumer profiling techniques is much appreciated, we believe that both audited gatekeepers and auditors/auditing organisations could benefit from practical guidance regarding the methodology and procedure of the audit, as referred to under Article 15, and the audit criteria.

2d. Proposed Auditing Framework

To help address this, we are providing a framework that helps determine primary guiding questions for performing such cooperative audits. These are not exhaustive, for we only intend to provide a starting point to facilitate rich multi-stakeholder discussion and deliberation on the topic. Derived from the typology developed by Koshiyama et al. (2022) and extensive industry experience, we offer a framework for algorithm audits that captures five key risk verticals: Robustness, Bias, Privacy, Explainability, and Efficacy.

Kindly note that we focus solely on the audit of algorithms in this public comment.

Risk Vertical	Guiding Questions	Audit Mechanisms
Robustness - the risk that the algorithm fails in unexpected circumstances or when under attack.	1. How can the risk of profiling techniques failing in expected circumstances be mitigated? 2. How can profiling techniques be safeguarded against adversarial attacks?	- Adversarial Testing - Red Teaming - Auditing model fallback plans
Bias - the risk that the algorithm treats individuals or groups unfairly.	1. How can the risk of profiling techniques discriminating against individuals on their protected characteristics be managed? 2. What are the safeguards and guardrails being implemented by gatekeepers to prevent filter bubbles, echo chambers and algorithmic overdependencies?	- Examining model outputs across different groups - Examining the use of protected characteristics and proxies - Examining model outputs across time - Gauging algorithmic bias across individual and group contexts
Privacy - the risk that the algorithm may leak sensitive or personal data.	1. How are gatekeepers ensuring algorithmic privacy?	- Compliance with privacy regulations (e.g., GDPR) and the

	2. Who has access to the data used by profiling algorithms? 3. What data minimisation practices are being followed to ensure that data collected and used for profiling purposes is relevant, adequate, and necessary for its purpose?	use of DPIAs (Data Protection Impact Assessment) - Ensuring cooperative audits follow data-access mechanisms wherein auditors have access to information such as model inputs, training data, and organisational processes - Ensuring platforms follow data minimisation and purpose limitation principles across product surfaces - Evaluating the deployment of Privacy Enhancing Technologies (PETs) such as dataset perturbation, differential privacy, federated learning, etc
Explainability/ interpretability - the risk that the system or its decisions may not be understandable to developers and users.	1. How, and according to which metrics, signals or criteria do profiling techniques create consumer profiles? 2. How can profiling techniques be developed and deployed in a manner that enables users to understand the decision-making procedure of the profiling? 3. What are the steps being taken by gatekeepers to explain algorithmic decision-making to users?	- Surveying community standards, with a particular focus on recommendation and feed guidelines - Stakeholder consultation - AI lifecycle monitoring for new deployments - Publication of resources or open-source code - Using appropriate methodologies to evaluate algorithmic explainability across model and dataset types
Efficacy - the risk that a system underperforms relative to its use case.	1. How often is the performance of profiling techniques examined? 2. Are there procedures for improving system performance?	- Use of performance metrics to gauge model accuracy, reproducibility, and reliability - User feedback mechanisms and procedures

3. Holistic AI resources

In lieu of the fact that the field of algorithm audits and assessments is relatively new, below we link some resources and references to our open-source and academic research.

1. Reducing AI Harms and Lawsuits through AI Governance, Risk Management and Compliance
2. Algorithm Auditing: Managing the Legal, Ethical, and Technological Risks of Artificial Intelligence, Machine Learning, and Associated Algorithms
3. AI Assurance Processes
4. A high-level overview of AI ethics
5. Holistic AI Open-source library

4. Concluding statement

Holistic AI welcomes the opportunity to provide comments on this important matter. We appreciate the open, transparent, and collaborative approach taken by the European Commission. We uphold the important objectives of the Digital Markets Act and stand ready to support National Authorities and the Commission in the implementation and enforcement of this important legislation.

Please contact publicpolicy@holisticai.com for any further information or follow-up on this submission.

Sincerely,
Holistic AI
https://www.holisticai.com/