Irish Council for
Civil Liberties

1st Floor
34 Usher's Quay
Dublin 8
T: +353 1 912 1640
E: info@iccl.ie
w: www.iccl.ie

European Commission DG CNECT A2

15 February 2022

Flaws in ex-post enforcement in the AI Act

Dear Mr. Gross,

1. We write on behalf of Irish Council for Civil Liberties (ICCL), Ireland's oldest independent human rights monitoring organisation. We suggest four enhancements to protect people and their rights in the draft EU regulation, Artificial Intelligence (AI) Act.[1]

2. We propose amendments to do the following:

   i. strengthen ex-post enforcement;
   ii. enhance assessments by moving beyond self-assessment by providers;
   iii. enhance redress and safeguards by giving complainants legal standing; and
   iv. empower Market Surveillance Authorities to act.

   Below, we elaborate on each.

3. Before we do so, we should make clear that ICCL has reservations on the question of whether product liability is the correct framework to protect fundamental rights under the Act.

Strengthen ex-post enforcement

4. The Commission's proposal assumes (emphasis added):

> "A comprehensive ex-ante conformity assessment through internal checks, combined with a ***strong ex-post enforcement***, could be an effective and reasonable solution for those

[1] Proposal for a Regulation of the European parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, 21 April 2021.

> systems, given the early phase of the regulatory intervention and the fact the AI sector is very innovative and expertise for auditing is only now being accumulated."[2]

5. However, "strong ex-post enforcement" is absent from the proposal. The proposal establishes a governance system with five tiers,[3] within which "market surveillance authorities" (MSAs) have the proactive investigatory function. Regulation (EU) 2019/1020 provides that MSAs independently decide when and what to investigate based on their assessment of risk.[4]

6. There are four problems:

   a. The Commission itself noted in its Communication of April 2021 that enforcement will be challenging because AI is not transparent.[5] It is therefore unclear how MSAs can effectively investigate complex AI matters such as fake content, manipulation, or bias.[6]

[2] Ibid. p. 14

[3] Five tiers

- The European Artificial Intelligence Board.
- National competent authorities shall ensure implementation of the regulation. One of these, a national supervisory authority, is designated by each Member State as the national contact for the European Commission and European Artificial Intelligence Board.
- Notifying authorities, which oversee conformity assessment bodies.
- Market surveillance authorities that already oversee product compliance in other areas.
- Conformity assessment bodies are third-party assessors.
- In practice, there might only be three tiers as Article 59 (2) says "The national supervisory authority shall act as notifying authority and market surveillance authority unless a Member State has organisational and administrative reasons to designate more than one authority."

[4] Regulation (EU) 2019/1020, Article 11 (3):

"In deciding on which checks to perform, on which types of products and on what scale, market surveillance authorities shall follow a risk-based approach taking into account the following factors:

(a) possible hazards and non-compliance associated with the products and, where available, their occurrence on the market;

(b) activities and operations under the control of the economic operator;

(c) the economic operator's past record of non-compliance;

(d) if relevant, the risk profiling performed by the authorities designated under Article 25(1);

(e) consumer complaints and other information received from other authorities, economic operators, media and other sources that might indicate non-compliance."

[5] "Fostering a European approach to Artificial Intelligence", European Commission, 21 April 2021 (URL: https://ec.europa.eu/newsroom/dae/redirection/document/75790), p. 6.

[6] A point well made by Michael Veale and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach." *Computer Law Review International* 22.4 (2021): 97-112. (URL: https://arxiv.org/abs/2107.03721). See particularly p. 108.

b. The Commission's assessment of the number of staff required at each Member State's MSA is far too small,[7] as should be evident from our experience of the GDPR.

c. The pressures on particular MSAs may be further exacerbated by forum-shopping providers from outside the Union opting for comparatively lax or under-resourced MSAs.[8]

d. MSAs will also have difficulty recruiting experts with adequate competence.

7. Many of these problems repeat those of GDPR enforcement.[9] Therefore, we recommend that the Commission reconvene the High-Level Expert Group to reflect on what is now known about enforcement in the parallel domain of data protection. The Expert Group may also wish to consider the value of an expert enforcement support capacity at EU level, and whether this should be attached to the European Artificial Intelligence Board.

Enhance assessments by moving beyond self-assessment by providers

8. It is no longer controversial to suggest that relying on self-regulation in the technology sector has led to significant harms that could otherwise have been avoided. Indeed, ICCLs recent experience of the self-regulatory provisions in the GDPR has again proven this.[10]

9. Despite this, the Act as proposed relies on providers to i) declare whether their systems are high-risk, ii) voluntarily provide information and manage risk,[11] and iii) inform authorities responsible for post-market monitoring.

[7] The Commission's explanatory memorandum in p. 12 estimates that "1 to 25 Full Time Equivalents per Member State" could be required. Across the 27 Member States of the Union, this estimate is 27-675 Full Time Equivalents.

[8] AI Act, Article 25 (1): "providers established outside the Union shall, by written mandate, appoint an authorised representative which is established in the Union."

[9] Johnny Ryan and Alan Toner, "Europe's Enforcement Paralysis", ICCL, September 2021 (URL: http://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf).

[10] For example, the Data Protection Impact Assessment provided for in Article 35 of the GDPR has been widely neglected in the online advertising industry. See Johnny Ryan, "GDPR enforcer rules that IAB Europe's consent popups are unlawful" ICCL, February 2022 (URL: https://www.iccl.ie/news/gdpr-enforcer-rules-that-iab-europes-consent-popups-are-unlawful/). Also see pp. 108-9, 117 in the decision from Belgian DPA (URL: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022-english.pdf). The various Facebook whistleblowers give a useful example, too.

[11] The only exception is biometric categorization in Annex III (1). Even for biometric categorization, self-assessment is considered sufficient when harmonized standards are established.

10. Moreover, Article 62 (1) says that providers must report serious problems to MSAs only after they have established "a causal link" between their AI systems and the incidents, or a reasonable likelihood of one. This allows providers to evade their responsibility by finding explanations that do not include their own AI systems, especially when these are part of a larger system.

11. We make two recommendations:

    a. The Act should require all providers of AI systems, not only those that claim to be providers of high-risk AI systems, to register in the public EU database[12] so that the uses and the users of the AI systems can be scrutinized by the public and by independent authorities such as notified bodies.

    b. Article 62 should require that operators report an incident or malfunction whenever an AI system is a part of the system concerned, and not only for serious incidents. This should include near-misses[13] so that other operators can learn from these incidents.

Enhance redress and safeguards by giving complainants legal standing

12. Although MSAs can receive information from "consumers" under Article 11 (3) (e) of Regulation (EU) 2019/1020, the Commission's proposed AI Act does not provide a mechanism for the public or organisations representing them to lodge formal complaints, or to enjoy attendant rights.[14]

13. Nor is there a right to judicial remedy against a provider or user for AI-specific harms or infringements of the Regulation.

14. The proposal therefore puts the primary burden of ex-post enforcement on MSAs, despite the high risk that MSA resources and powers envisaged by the Commission are unlikely to play the necessary role.

15. We make two recommendations:

[12] Article 60 of the AI Act.

[13] Incidents that if the circumstances were slightly different would have resulted in a "serious incident" as defined in Article 3 (44).

[14] As European data protection supervisory authorities note in "Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)", EDPS and EDPB, June 2021 (URL: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf).

a. Individuals and relevant representative organisations should be enabled to lodge complaints against AI operators.[15] Competent authorities should be obliged to act on these complaints within set timeframes. Complainants should have standing in that process.[16]

b. The proposal should provide individuals and representative organisations with an effective judicial remedy against "operators".[17]

Empower Market Surveillance Authorities to act

16. Chapter 3 of Title VIII, especially Article 64 (1) and (2), of the AI Act set out MSAs enforcement powers. These powers are much weaker than the minimum powers conferred on MSAs in Article 14 (4) of Regulation (EU) 2019/1020.

17. Article 14 (4) (d, e, j) of Regulation (EU) 2019/1020 have not been adapted to the AI Act. The MSAs should be empowered "to enter any premises",[18] "to reverse-engineer … to identify non-compliance and to obtain evidence",[19] and "to carry out unannounced on-site inspections"[20] of physical premises such as data centres. These powers should be adapted for AI systems so that inspections can be carried out remotely and unannounced.

18. Therefore, we recommend the following:

a. In addition to "unannounced on-site inspections and physical checks of products",[21] remote inspections should be explicitly and unambiguous provided for, since physical access may be unnecessary for certain AI systems.

b. The AI Act should empower MSAs to do so without notice, as they are empowered to do in other sectors.[22] Currently the proposal only provides that MSAs shall request access from providers. While using providers' Application Programming Interfaces ('API') [23] by arrangement with them may yield useful

[15] Similar to Article 77 and Article 80(2) of the GDPR.

[16] Similar to Article 57 (1) f of the GDPR.

[17] Similar to Article 79 of the GDPR.

[18] Article 14 (4) (e) of Regulation (EU) 2019/1020.

[19] Article 14 (4) (j) of Regulation (EU) 2019/1020.

[20] Article 14 (4) (d) of Regulation (EU) 2019/1020.

[21] Ibid.

[22] Ibid.

[23] Article 64 (1) of the AI Act.

information, it is important that MSAs retain their powers to investigate by independent means too, and without prior notice.

This is necessary to assess the resilience of AI systems "as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities"[24] and to check whether "measures to prevent and control for attacks"[25] have been taken by the operators.

19. We would be happy to meet with you and your team to discuss this.

On behalf of ICCL,

Dr Kris Shrishak

Technology Fellow

Dr Johnny Ryan

Senior Fellow

[24] Article 15 (4) of the AI Act.

[25] Ibid. "measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws."