Flaws in ex-post enforcement in the AI Act

Subject	EC proposed text	Council's text, 15 February 2022	ICCL's suggested amendments	Justification
1. Empower MSAs to act			**Article 64a NEW** **1. Market surveillance authorities shall, at a minimum, have the power to** **(a) carry out unannounced on-site and remote inspections of AI systems.** **(b) acquire samples related to AI systems, including through remote inspections, to reverse-engineer the AI systems and to acquire evidence to identify non-compliance.** **2. Member States may authorise their market surveillance authorities to reclaim from the relevant operator the totality of the costs of their activities with respect to instances of non-compliance.** **3. The costs referred to in paragraph 2 of this Article**	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. 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",[1] "to reverse-engineer … to identify non-compliance and to obtain evidence",[2] and "to carry out unannounced on-site inspections"[3] of physical premises such as data centres. Currently the proposal only provides that MSAs shall request access from providers. While using providers' Application Programming Interfaces ('API') by arrangement with them may yield useful information, it is important that MSAs retain their powers to investigate by independent means too, and without prior notice. We recommend that • remote inspections be explicitly and unambiguous provided for, since physical access may be unnecessary for certain AI systems. • MSAs be empowered to perform remote inspections without notice, as they are empowered to do in other sectors. 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"[4]

			may include the costs of carrying out testing, computation, hardware, storage, and the costs of activities relating to AI systems that are found to be non-compliant and are subject to corrective action prior to their placing on the market.	and to check whether "measures to prevent and control for attacks"[5] have been taken by the operators.
2. Monitor providers	**Annex VIII**		**Annex VIII (13) NEW the list of users of the AI systems**	The Commission's text relies on providers to i) declare whether their systems are high-risk, ii) voluntarily provide information and manage risk, and iii) inform authorities responsible for post-market monitoring. This is despite evidence 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.[6] 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 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.
	Article 51 Before placing on the market or putting into service a ~~**high-risk**~~ AI system ~~**referred to in Article 6(2)**~~, the provider or, where applicable, the authorised representative shall register that system in the EU database referred to in Article 60.	**Article 51** Before placing on the market or putting into service a ~~**high-risk**~~ AI system ~~**listed in Annex III referred to in Article 6(23**~~), the provider or, where applicable, the authorised representative shall register that system in the EU database referred to in Article 60.	**Article 51** Before placing on the market or putting into service a**n** AI system, the provider or, where applicable, the authorised representative shall register that system in the EU database referred to in Article 60.	
	Article 60 (1) The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraph 2 concerning ~~**high-risk**~~ AI systems ~~**referred to in Article 6(2)**~~ which are		**Article 60 (1)** The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraph 2 concerning AI systems which are registered in accordance with Article 51.	

	registered in accordance with Article 51.			
	Article 62 (1) Providers of high-risk AI systems placed on the Union market shall report any serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred. Such notification shall be made immediately ~~**after the provider has established a causal link between the AI system and**~~ the incident or malfunctioning ~~**or the reasonable likelihood of such a link**~~, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning.		**Article 62 (1)** Providers of high-risk AI systems placed on the Union market shall report any serious incident or any malfunctioning**, including near misses,** of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred. Such notification shall be made immediately **when an AI system is involved in** the incident or malfunctioning**, including near misses**, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning.	Article 62 (1) in the Commission's text 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. 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[7] so that other operators can learn from these incidents. This will also have broad societal benefit of helping operators identify and fix problems before a serious incident occurs.
	Article 17 (1) (i) procedures related to the reporting of serious	**Article 17 (1) (i)** procedures related to the reporting of serious	**Article 17 (1) (i)** procedures related to the reporting of serious	

	incidents and of malfunctioning in accordance with Article 62;	incidents and of malfunctioning in accordance with Article 62;	incidents and of malfunctioning**, including near misses,** in accordance with Article 62;	
	Article 29 (4) Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.	**Article 29 (4)** Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident~~ or any malfunctioning within the meaning of Article 62~~ and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.	**Article 29 (4)** Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning**, including near misses,** within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.	

[1] Article 14 (4) (e) of Regulation (EU) 2019/1020.
[2] Article 14 (4) (j) of Regulation (EU) 2019/1020.
[3] Article 14 (4) (d) of Regulation (EU) 2019/1020.
[4] Article 15 (4) of the AI Act.
[5] 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."
[6] 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.
[7] Incidents that if the circumstances were slightly different would have resulted in a "serious incident" as defined in Article 3 (44).

kris.shrishak@iccl.ie