

**AMENDMENT TO
RULES COMMITTEE PRINT 119-33
OFFERED BY MR. LATTA OF OHIO**

Add at the end of subtitle B of title XVII the following:

1 **SEC. 17___. COLLABORATION ON FRONTIER MODEL RISKS.**

2 (a) **ANTITRUST EXEMPTION.—**

3 (1) **IN GENERAL.—**It shall not be considered a
4 violation of any provision of the antitrust laws for—

5 (A) 2 or more non-Federal entities to pro-
6 vide or exchange information or assistance re-
7 lating to a covered artificial intelligence security
8 risk in good faith exclusively for a covered arti-
9 ficial intelligence security purpose; or

10 (B) 2 or more non-Federal entities to pro-
11 vide or exchange information or assistance for
12 the exclusive purpose of coordinating strategies
13 to reduce covered artificial intelligence security
14 risks via delaying or otherwise limiting the re-
15 lease, deployment, use, development, training,
16 testing, or evaluation of artificial intelligence,
17 provided that the non-Federal entities submit
18 prior written notice of the proposed coordinated

1 delay or limitation to the Attorney General and
2 the Federal Trade Commission, detailing the
3 specific covered artificial intelligence security
4 risk and the scope of the proposed restriction.

5 (2) LIMITATION.—Paragraph (1) shall not
6 apply to a non-Federal entity receiving information
7 or assistance unless the non-Federal entity uses such
8 information or assistance for a covered artificial in-
9 telligence security purpose and has implemented rea-
10 sonable internal controls to limit the extent to which
11 such information or assistance can be used for other
12 purposes.

13 (3) AFFIRMATIVE DEFENSE.—In any action or
14 proceeding brought under the antitrust laws, the ex-
15 emption provided under paragraph (1) shall con-
16 stitute an affirmative defense, and any non-Federal
17 entity claiming the exemption shall bear the burden
18 of proving by a preponderance of the evidence that
19 the entity's actions were taken in good faith and ex-
20 clusively for a purpose described in paragraph (1).

21 (4) RULE OF CONSTRUCTION.—Paragraph
22 (1)(A) shall not be construed to permit price-fixing,
23 allocating a market between competitors, monopo-
24 lizing or attempting to monopolize a market, boy-
25 cotting, or exchanges of price or cost information.

1 (5) EXEMPTION FROM DISCLOSURE.—Any in-
2 formation submitted to the Attorney General or the
3 Federal Trade Commission pursuant to paragraph
4 (1)(B), including any written notice submitted under
5 such paragraph and any information derived from
6 such submission that would reveal the substance of
7 such submission, shall be—

8 (A) used solely for the purpose of sub-
9 section (b);

10 (B) deemed voluntarily shared information
11 and exempt from disclosure under section 552
12 of title 5, United States Code; and

13 (C) withheld, without discretion, from the
14 public under section 552(b)(3) of title 5, United
15 States Code.

16 (b) INJUNCTIVE RELIEF.—

17 (1) IN GENERAL.—The Attorney General or the
18 Federal Trade Commission may seek, in a court of
19 competent jurisdiction, an injunction against the ini-
20 tiation or continuation of the provision or exchange
21 of information or assistance by non-Federal entities
22 described in subsection (a) that violates the antitrust
23 laws if the Attorney General or the Federal Trade
24 Commission determines that the non-Federal entities

1 are not acting in good faith or are otherwise unrea-
2 sonably engaging in anticompetitive acts.

3 (2) RULES OF CONSTRUCTION.—Nothing in
4 this section shall be construed to—

5 (A) create any immunity or exemption
6 from the antitrust laws if the Attorney General
7 or the Federal Trade Commission determines
8 that the non-Federal entities are not acting in
9 good faith or are otherwise unreasonably engag-
10 ing in anticompetitive acts; or

11 (B) to limit any private right of action for
12 any violation of the antitrust laws that is not
13 exempt under subsection (a).

14 (c) DEFINITIONS.—In this section:

15 (1) The terms “antitrust laws” and “non-Fed-
16 eral entity” have the meanings given those terms,
17 respectively, in section 102 of the Cybersecurity In-
18 formation Sharing Act of 2015 (6 U.S.C. 1501).

19 (2) The term “artificial intelligence” has the
20 meaning given that term in section 238(g) of the
21 John S. McCain National Defense Authorization Act
22 for Fiscal Year 2019 (10 U.S.C. 4001 note).

23 (3) The term “assistance” includes the provi-
24 sion of software, hardware, data, personnel, and
25 other resources.

1 (4) The terms “exclusive purpose” and “exclu-
2 sively for the purpose” mean that not more than an
3 insubstantial part of the use of the information or
4 assistance is for other purposes.

5 (5) The term “covered artificial intelligence se-
6 curity purpose” means the purpose of protecting
7 against, identifying, evaluating, testing, analyzing,
8 preventing, investigating, or mitigating a covered ar-
9 tificial intelligence security risk.

10 (6) The term “covered artificial intelligence se-
11 curity risk” means the potential for artificial intel-
12 ligence, including during development, training, test-
13 ing, evaluation, deployment, use, or release, to do 1
14 or more of the following:

15 (A) Substantially facilitate the development
16 or deployment of a chemical, biological, radio-
17 logical, nuclear, or offensive cyber weapon.

18 (B) Cause a disruption to, degradation of,
19 impairment of, or loss of operational control
20 over critical infrastructure that is reasonably
21 likely to result in a significant impact on secu-
22 rity, national economic security, national public
23 health or safety, or any combination thereof.

24 (C) Substantially reduce the ability of a
25 developer, deployer, owner, operator, user, eval-

1 uator, auditor, Federal department or agency,
2 or other governmental authority to oversee,
3 evaluate, monitor, control, contain, restrict ac-
4 cess to, disable, or terminate such artificial in-
5 telligence, if the applicable person or govern-
6 mental authority has authority or responsibility
7 to do so, including through unauthorized, de-
8 ceptive, evasive, or malicious activity involving
9 such artificial intelligence.

10 (D) Autonomously improve, or substan-
11 tially facilitate the autonomous improvement of
12 the capabilities of artificial intelligence in a
13 manner that creates a reasonable risk of a con-
14 sequence described in subparagraph (A), (B), or
15 (C).

16 (E) Be stolen, weaponized, trained, devel-
17 oped, or deployed by a covered nation (as de-
18 fined in section 4872(f)(2) of title 10, United
19 States Code) or an entity owned, controlled, or
20 directed by a covered nation in a manner that
21 poses a significant threat to the national secu-
22 rity, including through covert, clandestine, un-
23 disclosed, or otherwise concealed development
24 activities that attempt to evade detection or
25 verification.

1 (F)(i) Be vulnerable to unauthorized—

2 (I) access to or use of artificial intel-
3 ligence;

4 (II) extraction or copying of model
5 weights, parameters, or other nonpublic
6 model information;

7 (III) systematic querying or auto-
8 mated extraction designed to distill, rep-
9 licate, or reconstruct model capabilities; or

10 (IV) a compromise affecting the integ-
11 rity, reliability, or security of artificial in-
12 telligence, including through malicious
13 code, a backdoor, manipulated data, or
14 compromise of an artificial intelligence
15 model, training dataset, or artificial intel-
16 ligence component.

17 (ii) Where the access, use, extraction,
18 copying, querying, automated extraction, dis-
19 tillation, replication, reconstruction, or com-
20 promise described in clause (i)—

21 (I) creates a substantial risk of a con-
22 sequence described in subparagraphs (A)
23 through (D); or

24 (II) is for the benefit of, at the direc-
25 tion of, or under the control of—

1 (aa) a covered nation (as defined
2 in section 4872(f)(2) of title 10,
3 United States Code); or

4 (bb) an entity owned, controlled,
5 or directed by a covered nation.

