

.....
(Original Signature of Member)

118TH CONGRESS
2D SESSION

H. R. _____

To require the National Institute of Standards and Technology to establish task forces to facilitate and inform the development of technical standards and guidelines relating to the identification of content created by generative artificial intelligence, to ensure that audio or visual content created or substantially modified by generative artificial intelligence includes a disclosure acknowledging the generative artificial intelligence origin of such content, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Ms. ESHOO introduced the following bill; which was referred to the Committee
on _____

A BILL

To require the National Institute of Standards and Technology to establish task forces to facilitate and inform the development of technical standards and guidelines relating to the identification of content created by generative artificial intelligence, to ensure that audio or visual content created or substantially modified by generative artificial intelligence includes a disclosure acknowledging the generative artificial intelligence origin of such content, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Protecting Consumers
5 from Deceptive AI Act”.

6 **SEC. 2. FINDINGS.**

7 This Congress finds the following:

8 (1) The majority of Americans consume most of
9 their information online from social media platforms.
10 A 2023 Pew Research survey found that a large ma-
11 jority of U.S. adults (86%) say they often or some-
12 times get news from a smartphone, computer or tab-
13 let, including 56% who say they do so often.

14 (2) The increasing capabilities of generative ar-
15 tificial intelligence models has led to a marked in-
16 crease in the creation of convincing “deepfakes” and
17 greater difficulty for everyday Americans in telling
18 real and deepfake images, audio, and videos apart.
19 A December 2022 study found participants were
20 only 62% accurate when asked to determine whether
21 images were deepfake or real, and even worse, that
22 their self-reported confidence in their answers was
23 high, and unrelated to accuracy.

24 (3) Deepfakes create consumer deception issues,
25 where persons can create “deepfake” images and

1 videos to fool consumers about information related
2 to products they may wish to purchase. Fake celeb-
3 rity endorsements of various products and scams
4 have proliferated in the past year, including an ad
5 in which a deepfake of famous actor Tom Hanks en-
6 dored a dental insurance plan.

7 (4) The proliferation of deepfakes can also cre-
8 ate national security issues, such as a deepfake
9 image of an explosion at the Pentagon that was
10 shared widely last year and caused enough confusion
11 that the stock market briefly dipped.

12 (5) Deepfakes used in political advertising can
13 also create confusion, such as when someone used an
14 AI model that had been trained to replicate Presi-
15 dent Biden's voice was used to make robocalls to
16 voters in New Hampshire ahead of a primary elec-
17 tion, and provided false information intended to dis-
18 courage potential voters from voting in the election.
19 As the Supreme Court found 8-1 in *Citizens United*
20 *v. Federal Election Commission*, 558 U.S. 310
21 (2010), the government has an interest in
22 “‘insur[ing] that the voters are fully informed’
23 about the person or group who is speaking”.

24 (6) Requiring deepfakes to be clearly labeled is
25 important to protect consumers from deception, pro-

1 in identifying and labeling audio or visual con-
2 tent created or substantially modified by gen-
3 erative artificial intelligence, including exploring
4 interoperable standards that assist social media
5 and other online platforms with identifying,
6 maintaining, interpreting, and displaying water-
7 marks, digital fingerprinting, and secure con-
8 tent provenance metadata associated with audio
9 or visual content, while considering circumven-
10 tion techniques and enforcement.

11 (C) Supporting the development of tech-
12 nical standards and guidelines to identify and
13 label text-based content created or substantially
14 modified by generative artificial intelligence.
15 Such support may include developing standards
16 to embed content provenance data or metadata,
17 watermarking, digital fingerprinting, or other
18 technical measures when creating such content.

19 (2) STANDARDS BODIES.—To the extent pos-
20 sible, the outcome and output of the task forces es-
21 tablished pursuant to paragraph (1) should inform
22 development of technical standards developed by pri-
23 vate, consensus organizations, as referred to in sec-
24 tion 2 of the National Institute of Standards and

1 Technology Act (15 U.S.C. 272) and OMB Circular
2 A-119.

3 (3) MEMBERSHIP.—The Director of the Na-
4 tional Institute of Standards and Technology shall
5 include in the memberships of each of the task
6 forces described in paragraph (1) appropriate rep-
7 resentatives of the following:

8 (A) Relevant Federal agencies.

9 (B) Developers of generative artificial in-
10 telligence technology.

11 (C) Entities, including standards develop-
12 ment organizations, engaged in the development
13 of content detection standards and technology,
14 including authentication and traceability.

15 (D) Social networking service providers
16 and online instant messaging service providers.

17 (E) Online search engine service providers.

18 (F) Developers of web browsers and mobile
19 operating systems.

20 (G) Academic entities, civil society and ad-
21 vocacy groups, and other related entities, espe-
22 cially such entities and groups engaged in the
23 development or implementation of content de-
24 tection standards and technology.

25 (H) Privacy advocates and experts.

1 (I) Human rights lawyers and advocates
2 with expertise in the effects of technology in
3 countries around the world.

4 (J) Media organizations, including news
5 publishers and image providers.

6 (K) Creator associations and organizations
7 representing the interests of other copyright
8 owners.

9 (L) Artificial intelligence testing experts,
10 such as those with privacy expertise in artificial
11 intelligence red-teaming.

12 (M) Technical experts in digital forensics,
13 cryptography, and secure digital content and
14 delivery.

15 (N) Any other entity the Director deter-
16 mines appropriate.

17 (4) DUTIES.—

18 (A) SUBMISSION TO DIRECTOR.—Each of
19 the task forces established pursuant to para-
20 graph (1) shall, not later than 270 days after
21 the establishment of each such task force, sub-
22 mit to the Director of the National Institute of
23 Standards and Technology a report containing
24 recommendations relating to the technical

1 standards and guidelines each such task force is
2 supporting.

3 (B) SUBMISSION TO CONGRESS.—Each of
4 the task forces established pursuant to para-
5 graph (1) shall, not later than one year after
6 the establishment of each such task force and
7 annually thereafter for five years, submit to the
8 Committee on Science, Space, and Technology
9 and the Committee on Energy and Commerce
10 of the House of Representatives and the Com-
11 mittee on Commerce, Science, and Transpor-
12 tation of the Senate a report on the activities
13 of such task force for the immediately preceding
14 one year period.

15 (5) PRIVACY.—The task forces established pur-
16 suant to paragraph (1) shall consider issuing guid-
17 ance for online service and application providers and
18 operators to store and display content provenance
19 data and metadata in a privacy-preserving manner,
20 including clear guidance on how such providers and
21 operators can indicate to users when such users are
22 sharing content that contains content provenance
23 data and metadata, indicate the information con-
24 tained in the data and metadata such users are
25 sharing, and provide options to limit the data and

1 metadata such users are sharing that may have pri-
2 vacy implications.

3 (b) INFORMING CONSUMERS OF CONTENT GEN-
4 ERATED BY ARTIFICIAL INTELLIGENCE.—

5 (1) PROVIDERS OF GENERATIVE ARTIFICIAL IN-
6 TELLIGENCE APPLICATIONS.—A person who makes
7 available to users a software application based on
8 generative artificial intelligence technology shall—

9 (A) ensure that audio or visual content
10 created or substantially modified by such appli-
11 cation incorporates (as part of such content and
12 in a manner that may or may not be perceptible
13 by unaided human senses) a disclosure that—

14 (i) is machine-readable; and

15 (ii) acknowledges the generative artifi-
16 cial intelligence origin of such content;

17 (B) establish and implement reasonable
18 measures to prevent a disclosure described in
19 subparagraph (A) from being removed or other-
20 wise tampered with;

21 (C) collaborate with providers of covered
22 online platforms to assist such providers in
23 identifying and accessing the information of dis-
24 closures described in subparagraph (A); and

1 (D) ensure that such application makes
2 available to users the ability to incorporate,
3 within the metadata of content created or modi-
4 fied by such application, information regarding
5 the generative artificial intelligence origin of
6 such content, including tamper-evident informa-
7 tion regarding—

8 (i) the name of such application;

9 (ii) the name and version of the gen-
10 erative artificial intelligence model utilized
11 by such application to create or modify
12 such content;

13 (iii) the date and time associated with
14 the creation or modification of such con-
15 tent by such application; and

16 (iv) the portion of such content that
17 was created or modified by such applica-
18 tion.

19 (2) PROVIDERS OF COVERED ONLINE PLAT-
20 FORMS.—A person who makes available for use a
21 covered online platform—

22 (A) shall clearly and conspicuously provide
23 to a user of such platform, with respect to
24 audio or visual content accessed by such user
25 through such platform that incorporates a dis-

1 closure described in paragraph (1)(A), the in-
2 formation included in such disclosure; and

3 (B) may not, with respect to audio or vis-
4 ual content accessed by such user through such
5 platform that incorporates a disclosure de-
6 scribed in paragraph (1)(A), remove such dis-
7 closure or any incorporated information de-
8 scribed in paragraph (1)(D).

9 (3) REGULATIONS.—

10 (A) IN GENERAL.—Not later than 2 years
11 after the date of the enactment of this Act, the
12 Commission shall promulgate regulations under
13 section 553 of title 5, United States Code, to
14 carry out this subsection.

15 (B) CONSULTATION.—In carrying out sub-
16 paragraph (A), the Commission shall consult
17 with the National Institute of Standards and
18 Technology and the task forces established
19 under subsection (a)(1).

20 (4) ENFORCEMENT BY COMMISSION.—

21 (A) UNFAIR OR DECEPTIVE ACTS OR PRAC-
22 TICES.—A violation of this subsection or a reg-
23 ulation promulgated under this subsection shall
24 be treated as a violation of a regulation under
25 section 18(a)(1)(B) of the Federal Trade Com-

1 mission Act (15 U.S.C. 57a(a)(1)(B)) regarding
2 unfair or deceptive acts or practices.

3 (B) POWERS OF COMMISSION.—The Com-
4 mission shall enforce this subsection and the
5 regulations promulgated under this subsection
6 in the same manner, by the same means, and
7 with the same jurisdiction, powers, and duties
8 as though all applicable terms and provisions of
9 the Federal Trade Commission Act (15 U.S.C.
10 41 et seq.) were incorporated into and made a
11 part of this Act. Any person who violates such
12 subsection or a regulation promulgated under
13 such subsection shall be subject to the penalties
14 and entitled to the privileges and immunities
15 provided in the Federal Trade Commission Act.

16 (C) AUTHORITY PRESERVED.—Nothing in
17 this subsection may be construed to limit the
18 authority of the Commission under any other
19 provision of law.

20 (5) EFFECTIVE DATE.—Paragraphs (1) and (2)
21 of this subsection shall take effect on the date that
22 is 90 days after the date on which the regulations
23 promulgated under paragraph (3) take effect.

24 (6) SAFE HARBORS.—

1 (A) IN GENERAL.—A person who makes
2 available for use a generative artificial intel-
3 ligence application or a covered online platform
4 may satisfy the requirements of this subsection
5 (including regulations promulgated under this
6 subsection) by following self-regulatory guide-
7 lines that are approved by the Commission
8 under subparagraph (B).

9 (B) SELF-REGULATORY GUIDELINES.—

10 (i) INCENTIVES.—In promulgating
11 regulations under this subsection, the
12 Commission may provide incentives for
13 self-regulation.

14 (ii) DEEMED COMPLIANCE.—Incen-
15 tives described in clause (i) shall include
16 provisions for ensuring that a person will
17 be deemed to be in compliance with the re-
18 quirements of this subsection (including
19 regulations promulgated under this sub-
20 section) if that person complies with guide-
21 lines that, after provision of notice and an
22 opportunity for comment, are approved by
23 the Commission upon a determination that
24 such guidelines satisfy the requirements of

1 this subsection (including regulations pro-
2 mulgated under this subsection).

3 (iii) EXPEDITED RESPONSE TO RE-
4 QUESTS.—The Commission shall act upon
5 a request for approval of guidelines under
6 this paragraph not later than 180 days
7 after the date on which such request is
8 filed and shall set forth in writing conclu-
9 sions with regard to such request.

10 (C) APPEALS.—Final action by the Com-
11 mission on a request for approval of guidelines
12 under this paragraph, or the failure to act with-
13 in the time period described in subparagraph
14 (B)(iii), may be appealed to a district court of
15 the United States of appropriate jurisdiction as
16 provided for in section 706 of title 5, United
17 States Code.

18 (7) PRIVACY AND INTEROPERABILITY.—The
19 Commission shall consider privacy concerns and the
20 interoperability of standards when promulgating reg-
21 ulations under paragraph (3) and considering the
22 approval of guidelines under paragraph (6).

23 (c) DEFINITIONS.—In this section:

1 (1) AUDIO OR VISUAL CONTENT.—The term
2 “audio or visual content” means content in the form
3 of a digital image, a video, or audio.

4 (2) COMMISSION.—The term “Commission”
5 means the Federal Trade Commission.

6 (3) CONTENT PROVENANCE.—The term “con-
7 tent provenance” means the chronology of the origin
8 and history associated with digital content.

9 (4) COVERED ONLINE PLATFORM.—The term
10 “covered online platform” means a website, internet
11 application, or mobile application available to users
12 in the United States, including a social networking
13 site, video sharing service, search engine, or content
14 aggregation service available to users in the United
15 States, that—

16 (A) generates at least \$50,000,000 in an-
17 nual revenue; or

18 (B) had at least 25,000,000 monthly active
19 users for not fewer than 3 of the preceding 12
20 months.

21 (5) DIGITAL FINGERPRINTING.—The term
22 “digital fingerprinting” means the process by which
23 an identifier is derived from a piece of digital con-
24 tent and stored in a database, for the purpose of

1 identifying, matching against, or verifying such con-
2 tent, or similar content, at a later date.

3 (6) GENERATIVE ARTIFICIAL INTELLIGENCE.—

4 The term “generative artificial intelligence” means
5 the class of models and algorithms that use deep
6 learning algorithms or other statistical techniques to
7 generate new data that has similar characteristics
8 and properties to the data with respect to which
9 such models and algorithms have been trained, in-
10 cluding any form of digital content.

11 (7) MACHINE-READABLE.—The term “machine-
12 readable” has the meaning given such term in sec-
13 tion 3502 of title 44, United States Code.

14 (8) METADATA.—The term “metadata” has the
15 meaning given such term in section 3502 of title 44,
16 United States Code.

17 (9) WATERMARKING.—The term
18 “watermarking” means the act of embedding tam-
19 per-resistant information into digital content (per-
20 ceptibly or imperceptibly) which may be used to es-
21 tablish some aspect or aspects of the content prove-
22 nance of the content or to store reference informa-
23 tion.