

116TH CONGRESS
1ST SESSION

H. R. 4368

To prohibit the use of trade secrets privileges to prevent defense access to evidence in criminal proceedings, provide for the establishment of Computational Forensic Algorithm Standards, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 17, 2019

Mr. TAKANO introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Science, Space, and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To prohibit the use of trade secrets privileges to prevent defense access to evidence in criminal proceedings, provide for the establishment of Computational Forensic Algorithm Standards, 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 “Justice in Forensic
5 Algorithms Act of 2019”.

1 **SEC. 2. COMPUTATIONAL FORENSIC ALGORITHM STAND-**
2 **ARDS.**

3 (a) IN GENERAL.—Not later than 1 year after the
4 date of enactment of this Act, the Director of the National
5 Institute of Standards and Technology shall establish a
6 program to provide for creation and maintenance of stand-
7 ards for the development and use of computational foren-
8 sic software, to be known as the Computational Forensic
9 Algorithm Standards, consistent with the following:

10 (1) Standards shall include an assessment for
11 the potential for disparate impact, on the basis of
12 race, ethnicity, socioeconomic status, gender, and
13 other demographic features, in the development and
14 use of the computational forensic software.

15 (2) Standards shall address—

16 (A)(i) the underlying scientific principles
17 and methods implemented in computational fo-
18 rensic software; and

19 (ii) if, in the case of a particular method,
20 there are insufficient studies supporting its use,
21 what studies the Director has conducted to do
22 so, and the results of such studies;

23 (B) requirements for testing the software
24 including the conditions under which it needs to
25 be tested, types of testing data to be used, test-
26 ing environments, testing methodologies, and

1 system performance statistics required to be re-
2 ported including—

3 (i) accuracy, including false positive
4 and false negative error rates;

5 (ii) precision;

6 (iii) reproducibility;

7 (iv) robustness; and

8 (v) sensitivity;

9 (C) requirements for publicly available doc-
10 umentation by developers of computational fo-
11 rensic software of the purpose and function of
12 the software, the development process, including
13 source and description of training data, and in-
14 ternal testing methodology and results, includ-
15 ing source and description of testing data;

16 (D) requirements for laboratories and any
17 other entities using computational forensic soft-
18 ware to validate it for use, including to specify
19 the conditions under which the lab has vali-
20 dated it for their use, requirements for what in-
21 formation needs to be included in a public re-
22 port on the lab or other entity's validation, and
23 requirements for internal validation updates
24 when there are material changes to the soft-
25 ware; and

1 gorithm Testing Program and shall conduct an internal
2 validation according to the requirements outlined in the
3 Computational Forensic Algorithm Standards and make
4 the results publicly available. The internal validation shall
5 be updated when there is a material change in the soft-
6 ware that triggers a retesting by the Computational Fo-
7 rensic Algorithm Testing Program.

8 (d) REQUIREMENTS FOR TESTING.—The Director of
9 the National Institute of Standards and Technology shall
10 establish a Computational Forensic Algorithm Testing
11 Program, whose activities include the following:

12 (1) Testing individual software programs using
13 the testing requirements established in the Computa-
14 tional Forensic Algorithm Standards.

15 (2) Using realistic sample testing data similar
16 to what would be used by law enforcement in crimi-
17 nal investigations in performing such testing, includ-
18 ing incomplete and contaminated samples.

19 (3) Using testing data that represents diversity
20 of racial, ethnic, and gender identities and intersec-
21 tions of these identities in performing such testing.

22 (4) Using testing data that tests the limits of
23 the software and demonstrates the boundaries of re-
24 liability described in the performance measures de-

1 fined in the Computational Forensic Algorithm
2 Standards in performing such testing.

3 (5) Publishing the results of testing the soft-
4 ware online including results under conditions speci-
5 fied in the standards and across diversity of racial,
6 ethnic, and gender identities and intersections of
7 these identities in a publicly available format.

8 (e) TESTING FREQUENCY.—Retesting shall be con-
9 ducted when a material change is made to the software
10 that impacts its performance and may affect its outputs.
11 The Director shall establish requirements for determining
12 whether changes are material or nonmaterial.

13 (f) DISCOVERY IN CRIMINAL CASES.—Rule 16 of the
14 Federal Rules of Criminal Procedure is amended—

15 (1) in subdivision (a)(1), by adding at the end
16 the following:

17 “(H) *Use of Computational Forensic Soft-*
18 *ware.* Any results or reports resulting from
19 analysis by computational forensic software
20 shall be provided to the defendant, and the de-
21 fendant shall be accorded access to an execut-
22 able copy of the version of the computational
23 forensic software, as well as earlier versions of
24 the software, necessary instructions for use and
25 interpretation of the results, and relevant files

1 and data, used for analysis in the case and suit-
2 able for testing purposes. Such a report on the
3 results shall include—

4 “(i) the name of the company that de-
5 veloped the software;

6 “(ii) the name of the lab where test
7 was run;

8 “(iii) the version of the software that
9 was used;

10 “(iv) the dates of the most recent
11 changes to the software and record of
12 changes made, including any bugs found in
13 the software and what was done to address
14 those bugs;

15 “(v) documentation of procedures fol-
16 lowed based on procedures outlined in in-
17 ternal validation;

18 “(vi) documentation of conditions
19 under which software was used relative to
20 the conditions under which software was
21 tested; and

22 “(vii) any other information specified
23 by the Director of the National Institute of
24 Standards and Technology in the Com-

1 computational Forensic Algorithm Stand-
2 ards.”.

3 (g) INADMISSIBILITY OF CERTAIN EVIDENCE.—The
4 Federal Rules of Evidence are amended by adding at the
5 end of article I the following:

6 **“Rule 107. INADMISSIBILITY OF CERTAIN EVIDENCE THAT**
7 **IS THE RESULT OF ANALYSIS BY COMPUTA-**
8 **TIONAL FORENSIC SOFTWARE.**

9 “In any criminal case, evidence that is the result of
10 analysis by computational forensic software is admissible
11 only if—

12 “(1) the computational forensic software used
13 has been submitted to the Computational Forensic
14 Algorithm Testing Program of the Director of the
15 National Institute of Standards and Technology and
16 there have been no material changes to that software
17 since it was last tested; and

18 “(2) the developers and users of the computa-
19 tional forensic software agree to waive any and all
20 legal claims against the defense or any member of
21 its team for the purposes of the defense analyzing or
22 testing the computational forensic software.”.

23 (h) DEFINITIONS.—In this Act:

24 (1) COMPUTATIONAL FORENSIC SOFTWARE.—

25 The term “computational forensic software” means

1 software that relies on an automated or semiauto-
2 mated computational process, including one derived
3 from machine learning, statistics, or other data proc-
4 essing or artificial intelligence techniques, to process,
5 analyze, or interpret evidence.

6 (2) MATERIAL CHANGE.—The term “material
7 change” means an update to computational forensic
8 software that may affect the performance measures
9 defined in the Computational Forensic Algorithm
10 Standards or the use or output of the software.

11 (3) NONMATERIAL CHANGE.—The term “non-
12 material change” means an update to computational
13 forensic software that does not affect the perform-
14 ance measures, use, or output of the software.

○