I

117TH CONGRESS
1ST SESSION

H. R. 2438

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 Testing Standards and a Computational Forensic Algorithm Testing Program, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 8, 2021

Mr. TAKANO (for himself and Mr. EVANS) 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 Testing Standards and a Computational Forensic Algorithm Testing Program, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Justice in Forensic Algorithms Act of 2021".

SEC. 2. COMPUTATIONAL FORENSIC ALGORITHM TESTING STANDARDS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director of the National Institute of Standards and Technology shall establish a program to provide for creation and maintenance of standards for testing computational forensic software, to be known as the Computational Forensic Algorithm Testing Standards, consistent with the following:

(1) Testing standards shall include an assessment for the potential for disparate impact, on the basis of race, ethnicity, socioeconomic status, gender, and other demographic features.

(2) Testing standards shall address—

(A) the underlying scientific principles and methods implemented in computational forensic software; and

(B) requirements for testing the software including the conditions under which it needs to be tested, types of testing data to be used, testing environments, testing methodologies, and system performance statistics required to be reported including—

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

(ii) precision;

(iii) reproducibility;

(iv) robustness;

(v) sensitivity; and

(vi) system failure rates;

(C) requirements for publicly available documentation by developers of computational forensic software of the purpose and function of the software, the development process, including source and description of data used to develop the tool, and internal testing methodology and results, including source and description of testing data;

(D) requirements for laboratories and any other entities using computational forensic software to validate it for use, including to specify the conditions under which the lab has validated it for their use, requirements for what information needs to be included in a public report on the lab or other entity's validation, and requirements for internal validation updates when there are material changes to the software; and

(E) requirements for reports provided to defendants by prosecution produced docu-

menting the use and results of computational forensic software used in individual cases.

(3) Testing standards shall be issued as a rule-making under section 553 of title 5, United States Code.

(4) The Director shall consult with outside experts in forensic science, bioethics, algorithmic discrimination, data privacy, racial justice, criminal justice reform, exonerations, and other relevant areas of expertise identified through public input.

(b) PROTECTION OF TRADE SECRETS.—

(1) There shall be no trade secret evidentiary privilege to withhold relevant evidence in criminal proceedings in the United States courts.

(2) Nothing in this section may be construed to alter the standard operation of the Federal Rules of Criminal Procedure, or the Federal Rules of Evidence, as such rules would function in the absence of an evidentiary privilege.

(c) REQUIREMENTS FOR FEDERAL USE OF FORENSIC ALGORITHMS.—Any Federal law enforcement agency or crime laboratory providing services to a Federal law enforcement agency using computational forensic software may use only software that has been tested under the National Institute of Standards and Technology's Computa-

tional Forensic Algorithm Testing Program and shall conduct an internal validation according to the requirements outlined in the Computational Forensic Algorithm Testing Standards and make the results publicly available. The internal validation shall be updated when there is a material change in the software that triggers a retesting by the Computational Forensic Algorithm Testing Program.

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

(1) Testing individual software programs using the testing requirements established in the Computational Forensic Algorithm Testing Standards.

(2) Using realistic sample testing data similar to what would be used by law enforcement in criminal investigations in performing such testing, including incomplete and contaminated samples.

(3) Using testing data that represents diversity of racial, ethnic, and gender identities and intersections of these identities in performing such testing.

(4) Using testing data that tests the limits of the software and demonstrates the boundaries of reliability described in the performance measures de-

fined in the Computational Forensic Algorithm Testing Standards in performing such testing.

(5) Publishing the results of testing the software online including results under conditions specified in the testing standards and across diversity of racial, ethnic, and gender identities and intersections of these identities in a publicly available format.

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

(f) USE OF COMPUTATIONAL FORENSIC SOFTWARE.—Any results or reports resulting from analysis by computational forensic software shall be provided to the defendant, and the defendant shall be accorded access to both an executable copy of and the source code for the version of the computational forensic software—as well as earlier versions of the software, necessary instructions for use and interpretation of the results, and relevant files and data—used for analysis in the case and suitable for testing purposes. Such a report on the results shall include—

(1) the name of the company that developed the software;

(2) the name of the lab where test was run;

(3) the version of the software that was used;

(4) the dates of the most recent changes to the software and record of changes made, including any bugs found in the software and what was done to address those bugs;

(5) documentation of procedures followed based on procedures outlined in internal validation;

(6) documentation of conditions under which software was used relative to the conditions under which software was tested; and

(7) any other information specified by the Director of the National Institute of Standards and Technology in the Computational Forensic Algorithm Testing Standards.

(g) INADMISSIBILITY OF CERTAIN EVIDENCE.—In any criminal case, evidence that is the result of analysis by computational forensic software is admissible only if—

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

(2) the developers and users of the computational forensic software agree to waive any and all

legal claims against the defense or any member of its team for the purposes of the defense analyzing or testing the computational forensic software.

(h) DEFINITIONS.—In this Act:

(1) COMPUTATIONAL FORENSIC SOFTWARE.—The term ''computational forensic software'' means software that relies on an automated or semiautomated computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, to process, analyze, or interpret evidence.

(2) MATERIAL CHANGE.—The term ''material change'' means an update to computational forensic software that may affect the performance measures defined in the Computational Forensic Algorithm Testing Standards or the use or output of the software.

(3) NONMATERIAL CHANGE.—The term ''nonmaterial change'' means an update to computational forensic software that does not affect the performance measures, use, or output of the software.

○