H.R. 4368 – Justice in Forensic Algorithms Act of 2019 – Impact of Proposed Changes to Current Law

§	BILL TEXT	CURRENT STATUS	IMPACT OF CHANGE
	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. Trade secrets are protected by state and federal law, in order to promote scientific and other innovation.[1] 2. Defendants can already access probabilistic genotyping (PG) source code under confidentiality.[2] 3. PG testing standards have been in place for five years.[3]	1. Reduced forensic science innovation for criminal justice reliability and fairness. 2. No change in source code access to commercial PG software. 3. No change in PG testing standards.
	SEC. 2. COMPUTATIONAL FORENSIC ALGORITHM 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 (NIST) shall establish a program to provide for creation and maintenance of standards for the development and use of computational forensic software, to be known as the Computational Forensic Algorithm Standards, consistent with the following:	1. Robust PG standards based on scientific testing already exist.[3] 2. NIST promotes a foreign company over American innovators.[4] 3. PG computing replaces failed human review of DNA evidence.[5] 4. Failed human review of DNA evidence in past criminal cases.[6]	1. No change in PG standards. 2. Impartial judiciary replaced by unaccountable federal agency. 3. More DNA evidence failure, leading to criminal injustice. 4. No correction of failed DNA evidence interpretation in hundreds of thousands of criminal cases.

[1] All states in the U.S. have adopted some form of the 1979 Uniform Trade Secrets Act (UTSA), amended in 1985. In 2016, federal trade secret protection was strengthened by the Defend Trade Secrets Act (DTSA).

[2] Cybergenetics describes how defendants can access TrueAllele® technology source code in its "Access to TrueAllele® source code by defense experts" document. ESR's access policy is described in its "Access to STRmix™ software by defence legal teams." Source code is shared, and trade secret confidentiality is maintained.

[3] In 2015, the FBI's Scientific Working Group on DNA Analysis Methods (SWGDAM) issued "Guidelines for the validation of probabilistic genotyping systems."

[4] In 2016, Cybergenetics sent a "Letter to NIST" (available on Cybergenetics website) inquiring about NIST's commercial promotion of a foreign company.

[5] Validation studies demonstrating human failure and computer success in DNA casework include Perlin MW, Belrose JL, Duceman BW. "New York State TrueAllele® Casework validation study." *Journal of Forensic Sciences*. 2013;58(6):1458-66; and Perlin MW, Dormer K, Hornyak J, Schiermeier-Wood L, Greenspoon S. "TrueAllele® Casework on Virginia DNA mixture evidence: computer and manual interpretation in 72 reported criminal cases." *PLoS ONE*. 2014:9(3):e92837.

[6] See, for example: Perlin MW, "When DNA is not a gold standard: failing to interpret mixture evidence." *The Champion,* May, 2018; 42(4):50-56. The failed DNA mixture interpretation methods long promoted by NIST are inherently unreliable; see: Perlin MW. "Inclusion probability for DNA mixtures is a subjective one-sided match statistic unrelated to identification information." *Journal of Pathology Informatics*, 6(1):59, 2015.

H.R. 4368 – Justice in Forensic Algorithms Act of 2019 – Impact of Proposed Changes to Current Law

§	BILL TEXT	CURRENT STATUS	IMPACT OF CHANGE
a1	Standards shall include an assessment for the potential for disparate impact, on the basis of race, ethnicity, socioeconomic status, gender, and other demographic features, in the development and use of the computational forensic software.	PG gives a likelihood ratio (LR) that objectively measures identification information, accounts for ethnicity, and reduces disparate impact.[7]	Less PG innovation and reduced role of courts increases disparate impact on vulnerable groups.
a2	Standards shall address –	PG standards already exist.[8]	No change in PG standards.
a2Ai	the underlying scientific principles and methods implemented in computational forensic software; and	NIST has little expertise with PG principles and methods.[9]	Inexpert federal agency stifles impartial forensic science.
a2Aii	if, in the case of a particular method, there are insufficient studies supporting its use, what studies the Director has conducted to do so, and the results of such studies;	1. Sufficient studies by expert labs currently support DNA evidence.[10] 2. Peer-reviewed studies important.[11] 3. NIST lacks the relevant expertise to properly conduct PG testing studies.[9]	1. Decentralized forensic science expertise centralized in one agency. 2. Loss of peer-reviewed validations. 3. Effective PG testing by qualified scientists replaced by ineffective federal agency.
a2B	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 –	Appropriate PG testing standards have been in place for these purposes for five years.[3]	No change in standards.

[7] The ability of PG likelihood ratios to factor away racial and ethnic bias in DNA match statistics is described, for example, in Perlin MW, Legler MM, Spencer CE, Smith JL, Allan WP, Belrose JL, Duceman BW. "Validating TrueAllele® DNA mixture interpretation." *Journal of Forensic Sciences*. 2011;56(6):1430-1447.

[8] In addition to SWGDAM's 2015 validation guidelines,[3] the FBI has issued its 2020 "Quality assurance standards for forensic DNA testing laboratories."

[9] NIST's failure to understand basic PG principles was documented in a forensic conference talk: Perlin MW, "Getting past first Bayes with DNA mixtures," *American Academy of Forensic Sciences 66th Annual Meeting,* Seattle, WA, 2014, available on Cybergenetics' website.

[10] There have been 39 scientific validation studies done on Cybergenetics' TrueAllele® PG system, with at least as many conducted on ESR's STRmix™ PG system.

[11] Eight peer-reviewed TrueAllele validation studies include the four papers cited in other footnotes[5,7,16], as well as four additional papers: Perlin MW, Sinelnikov A. "An information gap in DNA evidence interpretation." *PLoS ONE*. 2009;4(12):e8327; Ballantyne J, Hanson EK, Perlin MW. "DNA mixture genotyping by probabilistic computer interpretation of binomially-sampled laser captured cell populations: combining quantitative data for greater identification information." *Science & Justice*. 2013;52(2):103-14; Perlin MW, Hornyak J, Sugimoto G, Miller K. "TrueAllele® genotype identification on DNA mixtures containing up to five unknown contributors." *Journal of Forensic Sciences*. 2015; 60(4):857-868; 2015;60(5):1263-1276; Bauer DW, Butt N, Hornyak JM, Perlin MW. "Validating TrueAllele® interpretation of DNA mixtures containing up to ten unknown contributors." *Journal of Forensic Sciences*. 2020;65(2):380-398.

§	BILL TEXT	CURRENT STATUS	IMPACT OF CHANGE
	(i) accuracy, including false positive and false negative error rates; (ii) precision; (iii) reproducibility; (iv) robustness; and (v) sensitivity;		
a2C	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 training data, and internal testing methodology and results, including source and description of testing data;	This PG information is currently provided by developers for use in court.[12]	No change in information.
a2D	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	This PG validation information is currently available.[13]	No change in validation.
a2E	requirements for reports provided to defendants by prosecution produced documenting the use and results of computational forensic software in individual cases.	This PG case information is currently provided.[14]	No change in information.
a3	Standards shall be issued as a rulemaking under section 553 of title 5, United States Code.	No comment.	No comment.
a4	The Director shall consult with outside experts in forensic science, bioethics, algorithmic discrimination, data privacy, racial justice, criminal	Such outside experts are already regularly consulted.	No change in expert consultation.

[12] Cybergenetics standard disclosure materials include a 4 GB DVD that provides DNA data, validation studies, scientific papers, admissibility rulings, no-cost access to the TrueAllele software, statistical model descriptions, and an opportunity for defendants to review computer source code.

[13] Cybergenetics documents and shares how its TrueAllele® Casework System complies with SWGDAM's PG validation guidelines.

[14] See the FBI's 2020 "Quality assurance standards for forensic DNA testing laboratories."

§	BILL TEXT	CURRENT STATUS	IMPACT OF CHANGE
	justice reform, exonerations, and other relevant areas of expertise identified through public input.		
b	PROTECTION OF TRADE SECRETS. — The Federal Rules of Evidence (FRE) are amended by adding at the end of article V the following:	1. Current practice can protect trade secrets to promote innovation.[1] 2. PG source code is available to defendants under confidentiality.[2]	1. PG companies may no longer innovate in forensic science. 2. No change in defendant access to source code.
b	**Rule 503. PROTECTION OF TRADE SECRETS IN A CRIMINAL PROCEEDING.** ‘‘In any criminal case, trade secrets protections do not apply when defendants would otherwise be entitled to obtain evidence.’’	1. Trade secret source code is not needed or used for scientific testing.[3] 2. Scientists test PG software; they do not have, read or use source code. 3. Source code is already available to defendants, subject to reasonable confidentiality restrictions.[2] 4. Defense teams may not disclose PG trade secrets to others.[1]	1. No change in how PG is tested or scientifically validated. 2. No scientific reliability benefit in having access to source code. 3. Innovators would lose technology protection that may result in a firm’s ceasing operation. 4. Defense teams could disclose PG trade secrets to others.
c	REQUIREMENTS FOR FEDERAL USE OF FORENSIC ALGORITHMS. — Any Federal law enforcement agency or crime laboratory providing services to a Federal agency using computational forensic software may use only software that has been tested under the National Institute of Standards and Technology’s Computational Forensic Algorithm Testing Program and shall conduct an internal validation according to the requirements outlined in the Computational Forensic Algorithm 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	1. Skilled and trained scientists test PG software for reliability.[3] 2. Broad diversity of PG testing from software developers, crime laboratories, and expert scientists.[14] 3. Impartial scientific testing of PG methods on DNA data determines reliability.[3,14] 4. Prosecutors and defenders are permitted to present DNA evidence that supports their case.[15]	1. NIST lacks the expertise needed to conduct PG testing properly.[9] 2. A single unaccountable federal agency would centralize PG testing. 3. An agency that favors some products and companies over others would be empowered to block reliable scientific evidence.[4] 4. Lawyers would need NIST approval to make their case using DNA evidence.

[15] See FRE Rule 702 on testimony by expert witnesses. For almost a century, judges have been gatekeepers, determining the admissibility of forensic evidence; see *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923). In federal (and most state) courts, judges weigh Daubert reliability factors of scientific testing, error rates, peer-review publication, existing standards, and general acceptance; see *Daubert v. Merrell Dow Pharmaceuticals* (92-102), 509 U.S. 579 (1993).

§	BILL TEXT	CURRENT STATUS	IMPACT OF CHANGE
	retesting by the Computational Forensic Algorithm Testing Program.		
d	REQUIREMENTS FOR TESTING. — The Director of the National Institute of Standards and Technology shall establish a Computational Forensic Algorithm Testing Program, whose activities include the following:	Testing of PG software is decentralized across hundreds of diverse groups, done by thousands of independent expert scientists who regularly conduct such testing.[3,10]	Testing of PG software would be centralized to a small partisan non-testing federal agency that does not generally conduct extensive testing, and lacks relevant expertise.
d1	Testing individual software programs using the testing requirements established in the Computational Forensic Algorithm Standards.	Current PG testing follows national validation standards.[8]	No change in validation standards. Testing done by an agency unskilled in the using the software programs.
d2	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.	Currently done.[5,7]	No change in testing standards.
d3	Using testing data that represents diversity of racial, ethnic, and gender identities and intersections of these identities in performing such testing.	Diversity is enhanced by having many groups conduct PG testing.[3]	Diversity is diminished by centralizing PG testing.
d4	Using testing data that tests the limits of the software and demonstrates the boundaries of reliability described in the performance measures defined in the Computational Forensic Algorithm Standards in performing such testing.	Currently done.[16]	No change in testing standards.
d5	Publishing the results of testing the software online including results under conditions specified in the standards and across diversity of racial, ethnic, and gender identities and intersections of these identities in a publicly available format.	Currently done.[17]	No change in sharing results.
e	TESTING FREQUENCY. — Retesting shall be conducted when a material change is made to the	Currently done.[14]	No change in retesting.

[16] See, for example, the validation paper: Greenspoon SA, Schiermeier-Wood L, Jenkins BC. "Establishing the limits of TrueAllele® Casework: a validation study." *Journal of Forensic Sciences*. 2015;60(5):1263-1276.

[17] See the websites of Cybergenetics and ESR for published studies that include validation results under such testing conditions.

§	BILL TEXT	CURRENT STATUS	IMPACT OF CHANGE
	software that impacts its performance and may affect its outputs. The Director shall establish requirements for determining whether changes are material or nonmaterial.		
f	DISCOVERY IN CRIMINAL CASES. — Rule 16 of the Federal Rules of Criminal Procedure is amended —	No comment.	No comment.
f1	in subdivision (a)(1), by adding at the end the following:	No comment.	No comment.
f1	''(H) *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 an executable copy of 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. This is already current practice for commercial PG software.[12] 2. No-cost access to PG software encourages scientific testing. 3. Executable software is entirely different from the source code text.	1. No change in the software information given to opposing side. 2. No change in software access, for either prosecution or defense. 3. No change in the irrelevancy of source code to scientific testing.
f1	''(i) the name of the company that developed the software; ''(ii) the name of the lab where test was run; ''(iii) the version of the software that was used; ''(iv) 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; ''(v) documentation of procedures followed based on procedures outlined in internal validation;	This information is currently provided to defendants.[12,14]	No change in reported information.

§	BILL TEXT	CURRENT STATUS	IMPACT OF CHANGE
	‘‘(vi) documentation of conditions under which software was used relative to the conditions under which software was tested; and ‘‘(vii) any other information specified by the Director of the National Institute of Standards and Technology in the Computational Forensic Algorithm Standards.’’		
g	INADMISSIBILITY OF CERTAIN EVIDENCE. — The Federal Rules of Evidence are amended by adding at the end of article I the following:	The courts decide the admissibility of scientific evidence.[15]	An unaccountable federal agency would decide admissibility.
g	**Rule 107. INADMISSIBILITY OF CERTAIN EVIDENCE THAT IS THE RESULT OF ANALYSIS BY COMPUTATIONAL FORENSIC SOFTWARE.** ‘‘In any criminal case, evidence that is the result of analysis by computational forensic software is admissible only if —	1. The FRE and well-established case law have long provided guidelines for judges to determine the admissibility of any and all evidence.[15] 2. The United States Constitution provides for separation of powers, and due process rights, assigning judicial functions to the Judiciary.[18]	1. Unjustified transfer of this responsibility for one specific type of scientific evidence from judges to an unaccountable federal agency. 2. Judicial powers and due process rights would be transferred away from an impartial Judiciary to an opaque Executive branch.
g	‘‘(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	1. Impartial judges decide on the admissibility of scientific evidence.[15] 2. The Judiciary branch is removed from commercial conflicts of interest. 3. Defense and prosecution have the right to introduce PG evidence.[18] 4. Independent scientists test methods and evidence, and report their results. 5. Forensic scientists testify in court. 6. Judges decide on the admissibility of evidence on a case-by-case basis.	1. An unaccountable federal agency would decide evidence admissibility. 2. NIST could further promote their favored PG companies and products. 3. Lawyers could not make their case without NIST approval. 4. One federal agency would replace thousands of forensic experts. 5. NIST does not provide testimony. 6. Courts could not weigh how reliably software is applied to data.

[18] The United Stated Constitution, Articles I, II & III, and Amendments 4, 5, 6 & 14.

H.R. 4368 – Justice in Forensic Algorithms Act of 2019 – Impact of Proposed Changes to Current Law

§	BILL TEXT	CURRENT STATUS	IMPACT OF CHANGE
g	‘‘(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.’’	Defense attorneys and experts are responsible for appropriately protecting trade secrets (and other sensitive information) that has been disclosed, subject to confidentiality restrictions or protective orders.[2]	Defense attorneys and experts would be free to publicly disclose highly confidential information that could cause irreparable harm to innovator companies, with no countervailing benefit to the justice system.
h	DEFINITIONS. — In this Act:	No comment.	No comment.
h1	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.	1. Different types of software are different in their transparency or bias. 2. Much non-forensic software falls within this overly broad definition. 3. PG software effects conventional unbiased statistical data analysis to find truth in DNA evidence.	1. All software would be lumped together, regardless of type. 2. NIST would regulate non-forensic software (e.g., Microsoft® Excel®). 3. Defendants could not challenge State-sponsored PG software, nor use their own PG alternatives.
h2	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 Standards or the use or output of the software.	No comment.	No comment.
h3	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.	No comment.	No comment.