GIBSON DUNN

U.S. Agencies Issue Pledge to Investigate AI Development and Use

Client Alert | April 11, 2024

The number of federal agencies that have joined the pledge and the scope of regulatory and enforcement priorities outlined in the joint statement are the strongest signals yet from the federal government that it intends to proactively monitor and regulate use cases of AI.

On April 4, 2024, the Department of Justice (DOJ) announced[1] that five additional cabinet-level federal agencies have joined a pledge to investigate unfair or discriminatory conduct involving artificial intelligence (AI). The joint statement—which was initially released in April 2023 by DOJ's Civil Rights Division, the Consumer Financial Protection Bureau, the Equal Employment Opportunity Commission, and the Federal Trade Commission—now includes the Department of Education, the Department of Health and Human Services, the Department of Homeland Security, the Department of Housing and Urban Development, and the Department of Labor. DOJ's Consumer Protection Branch also joined the pledge. The announcement follows an April 3, 2024 meeting of senior government officials to enhance coordination on AI-related issues. This was the second such meeting following President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, which directs federal agencies to use their authorities to prevent and address harms that may result from AI. These actions highlight federal agency efforts to coordinate and pursue actions using existing legal authorities. The addition of DOJ's Consumer Protection Branch to the pledge particularly signals the likelihood of new criminal investigations into AI-related conduct affecting consumers. Companies involved in the development and use of AI should be thoughtful about planning and avoidance of issues of concern identified in the pledge, including biased inputs, design opacity, and unintended uses. **The Pledge** The joint statement emphasizes the agencies' focus on their responsibility to ensure that automated systems are "developed and used in a manner consistent with existing federal laws." Signing agencies also pledge to "monitor the development and use of automated systems," promote responsible innovation, and "vigorously" protect individuals' rights. This pledge stems from Section 8 of the President's Executive Order, which directed federal agencies "to consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI."[2] **Agency Highlights** ***Existing Federal Laws Apply to AI***. The joint statement reiterates the view expressed in the initial April 2023 statement that the federal government believes that regulation of AI falls squarely within the ambit of existing federal laws and the agencies' collective authority to enforce civil rights, non-discrimination, fair competition, and consumer protection. Indeed, the statement declares that "existing legal authorities apply to the use of automated systems and innovative new technologies just as they apply to other practices." ***Emphasis on Unfair or Discriminatory Conduct***. As noted by DOJ in announcing the pledge:

> "Federal agencies are sending a clear message: we will use our collective authority and power to protect individual rights in the wake of increased reliance on artificial intelligence in various aspects of American life. As social media platforms, banks, landlords, employers and other businesses choose to rely on artificial intelligence, algorithms, and automated systems to conduct business, we stand ready to hold accountable those entities that fail to address the unfair and discriminatory outcomes that may result."[3]

This joint statement identifies the following particular issues of governmental concern with

Related People

Gustav W. Eyler

Svetlana S. Gans

Vivek Mohan

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

AI systems:

- **Data and Datasets**—The agency signers of the pledge note that automated system outcomes can be skewed by unrepresentative or imbalanced datasets, datasets that incorporate historical bias, or datasets that contain other types of errors. Making it clear that avoiding the use of protected characteristics as inputs is not enough, they also express concern that automated systems may correlate data with protected classes, which could lead to discriminatory outcomes.
- **Model Opacity and Access**—The agencies also worry that many automated systems are "black boxes" whose internal workings may not be clear even to the developer of the system. This lack of transparency, the agencies assert, could makes it more difficult for developers, businesses, and individuals to know whether an automated system is fair.
- **Design and Use**—Developers do not always understand or account for the contexts in which private or public entities will use their automated systems, the agencies state. Developers, they explain, may design a system on the basis of flawed assumptions about its users, relevant context, or the underlying practices or procedures it may replace.

Business Implications The number of federal agencies that have joined the pledge and the scope of regulatory and enforcement priorities outlined in the joint statement are the strongest signals yet from the federal government that it intends to proactively monitor and regulate use cases of AI. Other recent actions of note include the FTC's blanket authorization—which "will be in effect for 10 years"—of compulsory process in investigations of any products or services "that use or claim to be produced using artificial intelligence or claim to detect its use."[4] The Department of Justice also has established an Emerging Technology Board[5] and Chief AI Officer[6] to spearhead AI investigations and initiatives. Companies that develop or use AI (whether directly or indirectly) should take steps to ensure that they are compliant with federal law to the extent applicable to AI-related conduct in the absence of AI-specific requirements. In practice, this includes ensuring that AI systems and business processes that rely on AI are designed with compliance in mind and in accordance with an AI governance framework. Such framework should include, to the extent applicable, processes to stay aligned with current regulatory developments and priorities, including those identified in the pledge and accompanying joint statement. Gibson Dunn's leading AI, Privacy and Cybersecurity, and White Collar Investigations and Defense Practice Groups stand ready to help clients design and implement dynamic compliance programs and respond to agency actions. _____ [1] U.S. Department of Justice Office of Public Affairs, *Five New Federal Agencies Join Justice Department in Pledge to Enforce Civil Rights Laws in Artificial Intelligence*, April 4, 2024, available here. [2] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Sec. 8 (October 8, 2023), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/. [3] *Id.* [4] FTC, *FTC Authorizes Compulsory Process for AI-related Products and Services*, November 21, 2023, available at https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-authorizes-compulsory-process-ai-related-products-services. [5] *See* U.S. Department of Justice, *Deputy Attorney General Lisa Monaco Announcement*, November 9, 2023, available at https://www.justice.gov/opa/pr/readout-deputy-attorney-general-lisa-monacos-trip-new-york-and-connecticut [6] *See* U.S. Department of Justice, *Attorney General Garland Designates Jonathan Mayer to Serve as Chief AI Officer*, February 22, 2024, available at https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-designates-jonathan-mayer-serve-justice-departments-first.

The following Gibson Dunn attorneys assisted in preparing this update: Gustav W. Eyler, Svetlana S. Gans, Vivek Mohan, Rosemarie Ring, Alexander Southwell, and Jay Mitchell.

Gibson, Dunn & Crutcher's lawyers are available to assist in addressing any questions you may have regarding these issues. Please contact the Gibson Dunn lawyer with whom

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

you usually work, any leader or member of the firm's Artificial Intelligence, Privacy, Cybersecurity & Data Innovation, or White Collar Defense & Investigations practice groups, or the authors: Gustav W. Eyler – Washington, D.C. (+1 202.955.8610, geyler@gibsondunn.com) Svetlana S. Gans – Washington, D.C. (+1 202.955.8657, sgans@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com) Rosemarie T. Ring – San Francisco (+1 415.393.8247, rring@gibsondunn.com) Alexander H. Southwell – New York (+1 212.351.3981, asouthwell@gibsondunn.com) Jay Mitchell – Palo Alto (+1 650.849.5214, jmitchell@gibsondunn.com) **Artificial Intelligence**: Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com) Robert Spano – Paris/London (+33 1 56 43 14 07, rspano@gibsondunn.com) Eric D. Vandevelde – Los Angeles (+1 213.229.7186, evandevelde@gibsondunn.com) **Privacy, Cybersecurity and Data Innovation**: Ahmed Baladi – Paris (+33 1 56 43 13 00, abaladi@gibsondunn.com) S. Ashlie Beringer – Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com) Joel Harrison – London (+44 20 7071 4289, jharrison@gibsondunn.com) Jane C. Horvath – Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com) Rosemarie T. Ring – San Francisco (+1 415.393.8247, rring@gibsondunn.com) **White Collar Defense and Investigations**: Stephanie Brooker – Washington, D.C. (+1 202.887.3502, sbrooker@gibsondunn.com) Winston Y. Chan – San Francisco (+1 415.393.8362, wchan@gibsondunn.com) Nicola T. Hanna – Los Angeles (+1 213.229.7269, nhanna@gibsondunn.com) F. Joseph Warin – Washington, D.C. (+1 202.887.3609, fwarin@gibsondunn.com) © 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

Related Capabilities

Artificial Intelligence

Privacy, Cybersecurity, and Data Innovation

White Collar Defense and Investigations

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**