GIBSON DUNN

Artificial Intelligence and Automated Systems Legal Update (3Q22)

Client Alert | November 17, 2022

This quarter marked demonstrable progress toward sector-specific approaches to the regulation of artificial intelligence and machine learning ("AI"). As the EU continues to inch toward finalizing its draft Artificial Intelligence Act—the landmark, cross-sector regulatory framework for AI/ML technologies—the White House published a "Blueprint for an AI Bill of Rights," a non-binding set of principles memorializing the Biden administration's approach to algorithmic regulation. The AI Bill of Rights joins a number of recent U.S. legislative proposals, both at the federal and state levels,[1] and the Federal Trade Commission's ("FTC") Advanced Notice of Proposed Rulemaking to solicit input on questions related to potentially harmful data privacy and security practices, including automated decision-making systems.

Our 3Q22 Artificial Intelligence and Automated Systems Legal Update focuses on these regulatory efforts and also examines other policy developments within the U.S. and Europe.

I. U.S. REGULATORY & POLICY DEVELOPMENTS

A. AI Bill of Rights

The past several years have seen a number of new algorithmic governance initiatives take shape at the federal level, building on the December 2020 Trustworthy AI Executive Order that outlined nine distinct principles to ensure agencies "design, develop, acquire and use AI in a manner that fosters public trust and confidence while protecting privacy."[2]

On October 4, 2022—almost a year after announcing its development[3]—the White House Office of Science and Technology Policy ("OSTP") released a white paper titled "Blueprint for an AI Bill of Rights" intended to guide the design, use, and deployment of automated systems to "protect the American public in the age of artificial intelligence."[4] It provides practical guidance to government agencies and a call to action for technology companies, researchers, and civil society to build protections towards human-centric AI that is "designed to proactively protect [people] from harms stemming from unintended, yet foreseeable, uses or impacts of automated systems." The Blueprint identifies five non-binding principles to act as a "backstop" in order to minimize potential harms stemming from certain applications of AI:

- **Safe and Effective Systems**. To protect individuals from unsafe or ineffective systems, the Blueprint recommends proactive and ongoing consultation with the public and experts, risk identification and mitigation (which includes potentially not deploying a system or removing it from use), oversight mechanisms, and "adherence to domain-specific standards." The use of inappropriate, low-quality, or irrelevant data should be avoided, and data the AI system derives from other data should be identified and tracked to avoid feedback loops, compounded harms, and inaccurate results. AI systems should be subject to independent evaluations and reporting.

Related People

Frances Waldmann

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

- **Algorithmic Discrimination Protections**. AI systems should be designed and used in an equitable way and not discriminate on the basis of a characteristic protected by law. Systems should be subject to proactive equity and disparity assessments, reflect a representative and robust data set used for the development of AI, ensure accessibility for people with disabilities, and guard against the use of non-representative data or proxies that contribute to algorithmic discrimination. There should be independent evaluation of potential algorithmic discrimination and reporting, including making assessments public "whenever possible."
- **Data Privacy**. Individuals should have agency over how their data is used and should not be subject to surveillance. To that end, AI systems should process data consistent with data privacy principles, including privacy by design, data minimization, consents for collection, use, access, transfer and deletion of data, and proactively identifying and mitigating privacy risks. Systems should not use AI for design decisions that "obfuscate user choice or burden users with defaults that are privacy invasive." Surveillance and monitoring systems should be subject to heightened oversight, including an assessment of potential harms, and should not be used in contexts such as housing, education, or employment, or where the surveillance would monitor the exercise of democratic rights in a way that limits civil rights and liberties.
- **Notice and Explanation**. Designers, developers, and deployers of automated systems should provide generally accessible plain language documentation, including clear descriptions of the overall system functionality and the role automation plays, notice that such systems are in use, the individual or organization responsible for the system, and explanations of outcomes that are clear, timely, and accessible. Individuals should know how and why an outcome impacting them was determined by an automated system, including when the automated system is *not* the sole input determining the outcome. Automated systems should provide explanations that are technically valid, meaningful, useful, and calibrated to the level of risk.
- **Human Alternatives, Consideration, and Fallback**. People should be able to opt out of automated systems in favor of a human alternative, where appropriate, with a focus on ensuring broad accessibility and protecting the public from especially harmful impacts. There must be access to timely human consideration and remedy by a fallback and escalation process. Automated systems with an intended use within sensitive domains (e.g., criminal justice, employment, education, and health) should additionally be tailored to the purpose, provide meaningful access for oversight, include training for any people interacting with the system, and incorporate human consideration for adverse or high-risk decisions.

The principles apply broadly to " automated systems that … have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services." "Automated systems" are themselves defined very broadly, encompassing essentially any system that makes decisions using computation.[5] The Blueprint is intended to further the ongoing discussion regarding privacy among federal government stakeholders and the public, but its impact on the private sector is likely to be limited because—unlike the wide-ranging EU AI Act, which is inching towards an implementation date—it lacks prohibitions on AI deployments and details or mechanisms for enforcement. The Blueprint is accompanied by supporting documentation, including a set of real-life examples and a high-level articulation of how the five principles can "move into practice."[6]

B. FTC Rulemaking on "Harmful Commercial Surveillance and Lax Data Security"

On August 11, 2022, the FTC announced an Advance Notice of Proposed Rulemaking

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

("ANPRM") to seek public comment on data privacy and security practices ("commercial surveillance") that harm consumers.[7] Specifically, the FTC invites comment on "whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive."[8]

Notably, the ANPRM also solicits public input on algorithmic decision-making, including the prevalence of algorithmic error, discrimination based on protected categories facilitated by algorithmic decision-making systems, and how the FTC should address algorithmic discrimination through the use of proxies.[9] On September 27, the FTC continued the rulemaking process by hosting a virtual "Commercial Surveillance and Data Security Public Forum (the "Public Forum")" to gather public feedback on the proposed rulemaking.[10]

The FTC is undertaking this rulemaking under Section 18 of the FTC Act (also known as "Magnuson-Moss"),[11] a lengthy and complicated hybrid rulemaking process that goes beyond the Administrative Procedure Act's standard notice-and-comment procedures.[12] In light of these procedural hurdles, any new proposed rules likely will take considerable time to develop. The ANPRM notes that, if new rules are not forthcoming, the record developed in response to the ANPRM nevertheless will "help to sharpen the Commission's enforcement work and may inform reform by Congress or other policymakers." The inclusion of algorithmic decision-making in the scope of the potential rulemaking underscores the FTC's continued focus on taking the lead in the regulation of automated systems at federal level.[13]

C. National Institute of Standards and Technology ("NIST")

On August 18, 2022, NIST published and sought comments on a second draft of the NIST Artificial Intelligence Risk Management Framework ("AI RMF").[14] The AI RMF, as mandated by Congress, is intended for voluntary use to help incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.[15] NIST plans to publish AI RMF in January 2023. NIST also sought comments on the draft NIST AI RMF Playbook, an online resource providing recommended actions on how to implement the AI RMF.

D. New York City Artificial Intelligence Law

On September 19, 2022, the New York City Department of Consumer and Worker Protection ("DCWP") proposed rules in an attempt to clarify numerous ambiguities in New York City's AI law, which takes effect on January 1, 2023.[16]

New York City's law will restrict employers from using AEDT in hiring and promotion decisions unless it has been the subject of a bias audit by an "independent auditor" no more than one year prior to use.[17] The law also imposes certain posting and notice requirements to applicants and employees. The DCWP's proposed rules are currently under consideration and may well invite more questions than answers as uncertainty about the requirements lingers. The proposed rules attempt to clarify certain key terms, specify the requirements for and provide examples of bias audits, and outline several different ways by which, if passed, employers may provide the advance notice to candidates and employees regarding the use of an AEDT.[18]

A public hearing was held on November 4, 2022, and the record for comments is now closed, but DCWP has not provided a firm date on which the proposed rules will be finalized. We will continue to monitor further guidance that will emerge as the January 1, 2023 effective date nears.

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

II. INTELLECTUAL PROPERTY

A. Federal Circuit Rules Inventors Must Be Natural Human Beings

On August 11, 2022, The U.S. Court of Appeals for the Federal Circuit affirmed a lower court's ruling in *Thaler v. Vidal* that the plain text of the Patent Act requires that inventors must be human beings.[19] Attorneys for Steven Thaler, the creator of the AI system "DABUS" (Device for the Autonomous Bootstrapping of Unified Sentience), argued that an AI system that has "created" several inventions should be granted a patent application, and that inventorship requirements should not be a bar to patentability. The argument followed the U.S. Patent and Trademark Office's rejection of two DABUS patent applications. A Virginia federal court affirmed that ruling last year, finding AI cannot be an inventor under U.S. patent law.[20] The DABUS project has also lodged several unsuccessful test cases in Australia, the EU, and the UK.[21]

III. EU REGULATORY & POLICY DEVELOPMENTS

A. AI Act Developments

Following the agreement on a common European AI strategy in 2018, the establishment of a high-level expert group in 2019, and various other publications, including a 2020 White Paper, on April 21, 2021, the EU Commission published its proposal for "the world's first legal framework on AI"—the EU Artificial Intelligence Act ("AI Act").[22] In September 2022, the Czech Presidency of the Council of the European Union published a new proposal and may be on the cusp of finalizing the text for the proposed AI Act.[23] The recent proposed changes to the draft legislation were relatively minor but notably included narrowing the definition of AI to focus on an AI system's degree of autonomy and adding a chapter on General Purpose AI ("GPAI")—large, multipurpose data models—indicating that obligations for these systems will likely be imposed through an implementing act.

The Committee of the Permanent Representatives of the Governments of the Member States to the European Union is expected to approve the final version on November 18, 2022, before ministers in the Transport, Telecommunications and Energy Council sign off on December 6, 2022.[24]

B. Draft AI Liability Directive and New Draft Product Liability Directive

On September 28, 2022, the European Commission ("EC") published a set of proposals aiming to modernize the EU's existing liability regime and adapt it to AI systems, give businesses legal certainty, and harmonize member states' national liability rules for AI. The EC had previewed the draft rules in its February 2020 Report on Safety and Liability, emphasizing the specific challenges posed by AI products' complex, opaque, and autonomous characteristics.[25] The draft EU AI Act, the AI Liability Directive ("ALD") [26] and the updated Product Liability Directive ("PLD")[27] are intended to be complementary[28] and, together, are set to significantly change liability risks for developers, manufacturers and suppliers who place AI-related products on the EU market.[29]

The draft Product Liability Directive ("PLD") establishes a framework for *strict liability* for defective products across the EU—including AI systems—meaning claimants need only show that harm resulted from the use of a defective product. Notably, the mandatory safety requirements set out in the draft AI Act can be taken into account by a court for the purpose of determining whether a product is defective.

The AI Liability Directive (ALD"), which would apply to *fault-based liability* regimes in the EU, would create a rebuttable "presumption of causality" against any AI system's

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

developer, provider, or user, and would make it easier for potential claimants to access information about specific "High-Risk" AI Systems—as defined by the draft EU AI Act. Of particular significance to companies developing and deploying AI-related products is the new disclosure obligation related to "High-Risk" AI systems, which could potentially require companies to disclose technical documentation, testing data, and risk assessments—subject to safeguards to protect sensitive information, such as trade secrets. Failure to produce such evidence in response to a court order would permit a court to invoke a presumption of breach of duty.

The PLD and ALD will be subject to review and approval by the European Council and Parliament before taking effect. Once implemented, Member States will have two years to implement the requirements into local law. We are monitoring developments closely and stand ready to assist clients with preparing for compliance with the emerging EU AI regulatory framework.

IV. UK REGULATORY AND POLICY DEVELOPMENTS

A. UK Unveils Data Reform Bill, Proposes Approach to AI Regulation

On July 18, 2022, the UK government introduced several data reform initiatives aimed at guiding responsible use of data while promoting innovation, and regulating the use of AI.

The Data Protection and Digital Information Bill ("DPDI"),[30] which includes measures to "use AI responsibly while reducing compliance burdens on businesses to boost the economy," is now facing delays[31] and a new public consultation, but would, if enacted, amend the current rules on data protection and privacy, including AI. As introduced, DPDI clarifies the circumstances in which organizations can use automated decision-making. If a decision produces a legal or similarly significant effect for an individual and involves the processing of sensitive "special category" data, it cannot (other than in very specific circumstances) be taken solely on an "automated decision basis" with no "meaningful" human involvement. Otherwise, automated decision-making systems can be used, subject to safeguards intended to "protect the rights and freedoms of the individual." These safeguards include requirements that the organization deploying the automated decision-making system can provide information about the decisions and provide individuals about whom a decision is being made with an opportunity to make representations about the decision, escalate to human intervention, and contest any decisions.

In parallel with the new legislation, the government also released a set of policy initiatives outlining the government's approach to regulating AI in the UK, reiterating a commitment to sector-specific regulation and a "less centralized approach than the EU."[32] Its "AI Action Plan" highlights the UK government's "focus on supporting growth and avoiding unnecessary barriers being placed on businesses," emphasizing that the proposal will "allow different regulators to take a tailored approach to the use of AI in a range of settings . . . [which] better reflects the growing use of AI in a range of sectors."[33] The guidance sets out six core principles, which require developers and users to: (1) ensure that AI is used safely; (2) ensure that AI is technically secure and functions as designed; (3) make sure that AI is appropriately transparent and explainable; (4) consider fairness; (5) identify a legal person to be responsible for AI; and (6) clarify routes to redress or contestability.

A range of regulators—Ofcom, the Competition and Markets Authority, the Information Commissioner's Office, the Financial Conduct Authority, and the Medicine and Healthcare Products Regulatory Agency—will be asked to interpret and implement the principles and encouraged to consider "lighter touch options which could include guidance and voluntary measures or creating sandboxes."[34]

B. UK ICO Publishes Guidance on Privacy Enhancing Technologies

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

On September 7, 2022, the UK Information Commissioner's Office ("ICO") published draft guidance on privacy-enhancing technologies ("PETs") intended to "help organisations unlock the potential of data by putting a data protection by design approach into practice."[35] PETs are technologies that are intended to help organizations share and use people's data responsibly, lawfully, and securely, including by minimizing the amount of data used and by encrypting or anonymizing personal information.

The ICO's draft PETs guidance explains the benefits and different types of PETs currently available, as well as how they can help organizations comply with data protection law. For example, the guidance contains information on the benefits and risks of using synthetic data to train large models. This guidance forms part of the ICO's draft guidance on anonymization and pseudonymization, and the ICO is seeking feedback to help refine and improve the final guidance.

---

[1] *See, e.g.*, the American Data Privacy Protection Act ("ADPPA"), which would require certain types of businesses developing and operating AI to undertake risk assessments. For more details, please see our Artificial Intelligence and Automated Systems Legal Update (2Q22).

[2] For more details, please see President Trump Issues Executive Order on "Maintaining American Leadership in Artificial Intelligence."

[3] White House, *Join the Effort to Create a Bill of Rights for an Automated Society* (Nov. 10, 2021), available at https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/.

[4] White House, Office for Science and Technology, available at https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[5] "An "automated system" is any system, software, or process that uses computation as whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or otherwise interact with individuals and/or communities. Automated systems include, but are not limited to, systems derived from machine learning, statistics, or other data processing or artificial intelligence techniques, and exclude passive computing infrastructure. "Passive computing infrastructure" is any intermediary technology that does not influence or determine the outcome of decision, make or aid in decisions, inform policy implementation, or collect data or observations, including web hosting, domain registration, networking, caching, data storage, or cybersecurity. Throughout this framework, automated systems that are considered in scope are only those that have the potential to meaningfully impact individuals' or communities' rights, opportunities, or access." *See* The White House, OSTP, Blueprint for an AI Bill of Rights, *Definitions*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/definitions/.

[6] The White House, OSTP, Blueprint for an AI Bill of Rights, *From Principles to Practice*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/safe-and-effective-systems-3/.

[7] Federal Register, *Trade Regulation Rule on Commercial Surveillance and Data Security*, https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

[8] *Id*.

[9] Public comments are available at https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

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

[10] For more details, please see FTC Launches Commercial Surveillance and Data Security Rulemaking, Holds a Public Forum, and Seeks Public Input.

[11] Magnuson-Moss Warranty Federal Trade Commission Improvement Act, 15 U.S.C. § 57a(a)(1)(B).

[12] The FTC may promulgate a trade regulation rule to define acts or practices as unfair or deceptive "only where it has reason to believe that the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent." The FTC may make a determination that unfair or deceptive acts or practices are prevalent only if: "(A) it has issued cease and desist orders regarding such acts or practices, or (B) any other information available to the Commission indicates a widespread pattern of unfair or deceptive acts or practices." That means that the agency must show (1) the prevalence of the practices, (2) how they are unfair or deceptive, and (3) the economic effect of the rule, including on small businesses and consumers.

[13] For more detail on the FTC's activities in this space, please see our 2021 Artificial Intelligence and Automated Systems Annual Legal Review.

[14] NIST Seeks Comments on AI Risk Management Framework Guidance, Workshop Date Set, https://www.nist.gov/news-events/news/2022/08/nist-seeks-comments-ai-risk-management-framework-guidance-workshop-date-set; NIST, *AI Risk Management Framework: Second Draft*, https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf.

[15] NIST Risk Management Framework, https://www.nist.gov/itl/ai-risk-management-framework.

[16] NYC Dep't Consumer & Worker Prot., Notice of Public Hearing and Opportunity to Comment on Proposed Rules, https://rules.cityofnewyork.us/wp-content/uploads/2022/09/DCWP-NOH-AEDTs-1.pdf.

[17] For more details, please see Gibson Dunn's New York City Enacts Law Restricting Use of Artificial Intelligence in Employment Decisions.

[18] For more details regarding the proposed rules, please see Gibson Dunn's New York City Proposes Rules to Clarify Upcoming Artificial Intelligence Law for Employers.

[19] *Thaler v. Vidal*, 43 F.4th 1207 (Fed. Cir. 2022).

[20] *Thaler v. Hirshfeld*, 558 F. Supp. 3d 238 (E.D. Va. 2021).

[21] *See, e.g.*, 2021 Artificial Intelligence and Automated Systems Annual Legal Review.

[22] For more details, please see 2021 Artificial Intelligence and Automated Systems Annual Legal Review.

[23] EURActiv, *AI Act: Czech EU presidency makes final tweaks ahead of ambassadors' approval* (Nov. 4, 2022), https://www.euractiv.com/section/digital/news/ai-act-czech-eu-presidency-makes-final-tweaks-ahead-of-ambassadors-approval/.

[24] Euractiv, *Last-minute changes to EU Council's AI Act text ahead of general approach* (Nov. 14, 2022), available at https://www.euractiv.com/section/digital/news/last-minute-changes-to-eu-councils-ai-act-text-ahead-of-general-approach/.

[25] EC, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM(2020) 64 (Feb. 19, 2020), available at

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

https://ec.europa.eu/info/files/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics_en; *see also* European Commission, *Questions & Answers: AI Liability Directive*, available at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5793 ("Current national liability rules are not equipped to handle claims for damage caused by AI-enabled products and services. In fault-based liability claims, the victim has to identify whom to sue, and explain in detail the fault, the damage, and the causal link between the two. This is not always easy to do, particularly when AI is involved. Systems can oftentimes be complex, opaque and autonomous, making it excessively difficult, if not impossible, for the victim to meet this burden of proof.")

[26] European Commission, *Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence* (Sept. 28, 2022), available at https://ec.europa.eu/info/files/proposal-directive-adapting-non-contractual-civil-liability-rules-artificial-intelligence_en.

[27] European Commission, *Proposal for a directive of the European Parliament and of the Council on liability for defective products* (Sept. 28, 2022), available at https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en.

[28] The AI Liability Directive uses the same definitions as the AI Act, keeps the distinction between high-risk/non-high risk AI, recognizes the documentation and transparency requirements of the AI Act by making them operational for liability through the right to disclosure of information, and incentivizes providers/users of AI-systems to comply with their obligations under the AI Act.

[29] European Commission, *Questions & Answers: AI Liability Directive*, available at https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5793 ("Together with the revised Product Liability Directive, the new rules will promote trust in AI by ensuring that victims are effectively compensated if damage occurs, despite the preventive requirements of the AI Act and other safety rules.").

[30] Data Protection and Digital Information Bill, available at https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf.

[31] Spencer, M. (2022, September 5). Business Statement [Hansard]. (Vol. 719), available at https://hansard.parliament.uk/commons/2022-09-05/debates/FB4997E6-14A2-4F25-9472-E2EE7F00778A/BusinessStatement ("the Government will not move the Second Reading and other motions relating to the Data Protection and Digital Information Bill today to allow Ministers to consider the legislation further").

[32] Gov.UK, Press Release, *UK sets out proposals for new AI rulebook to unleash innovation and boost public trust in the technology*, available at https://www.gov.uk/government/news/uk-sets-out-proposals-for-new-ai-rulebook-to-unleash-innovation-and-boost-public-trust-in-the-technology.

[33] *Id*.

[34] *Id*.

[35] ICO, *ICO publishes guidance on privacy enhancing technologies* (Sept. 7, 2022), available at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/. *See also* https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf.

The following Gibson Dunn lawyers prepared this client update: H. Mark Lyon, Frances Waldmann, and Emily Lamm.

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

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, any member of the firm's Artificial Intelligence and Automated Systems Group, or the following authors:

H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com) Frances A. Waldmann - Los Angeles (+1 213-229-7914,fwaldmann@gibsondunn.com)

Please also feel free to contact any of the following practice group leaders and members:

Artificial Intelligence and Automated Systems Group: J. Alan Bannister – New York (+1 212-351-2310, abannister@gibsondunn.com) Patrick Doris – London (+44 (0)20 7071 4276, pdoris@gibsondunn.com) Cassandra L. Gaedt-Sheckter – Co-Chair, Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com) Kai Gesing – Munich (+49 89 189 33 180, kgesing@gibsondunn.com) Joel Harrison – London (+44(0) 20 7071 4289, jharrison@gibsondunn.com) Ari Lanin – Los Angeles (+1 310-552-8581, alanin@gibsondunn.com) Carrie M. LeRoy – Palo Alto (+1 650-849-5337, cleroy@gibsondunn.com) H. Mark Lyon – Co-Chair, Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com) Vivek Mohan – Co-Chair, Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com) Alexander H. Southwell – New York (+1 212-351-3981, asouthwell@gibsondunn.com) Christopher T. Timura – Washington, D.C. (+1 202-887-3690, ctimura@gibsondunn.com) Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com) Michael Walther – Munich (+49 89 189 33 180, mwalther@gibsondunn.com)

© 2022 Gibson, Dunn & Crutcher LLP Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.

Related Capabilities

Artificial Intelligence

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