Hashed & Salted | A Privacy and Data Security Update
June 2022

Staying Ahead of AI Regulations—What Businesses Need to Know About the Current Regulatory, Legislative And Operational Trends

An increasing spotlight on artificial intelligence and machine learning (collectively, AI) in the U.S., in particular around the concern that AI causes consumer harm, such as discrimination and unconscious bias, indicates that monitoring and regulating AI is a priority for many lawmakers and regulators.

We are seeing an acceleration of federal and state legislative and regulatory focus on artificial intelligence and machine learning (collectively, AI) in the U.S. around the increasing concern that AI causes consumer harm, such as discrimination and unconscious bias. This increasing spotlight on AI indicates that monitoring and regulating AI is a priority for many lawmakers and regulators, and understanding these legal impacts must be a priority for all who build, use, purchase or test AI. For the purposes of this article, we have defined the term AI to mean "a process, derived from machine learning or artificial intelligence techniques, that makes or facilitates a decision or facilitates human decision-making with respect to covered data, including to determine the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual." This definition is from the proposed 2022 American Privacy and Data Protection Act.

Federal Artificial Intelligence Developments

Proposed Federal Privacy Legislation Signaling New Data Rights and AI Review Requirement

Congress introduced bipartisan federal privacy legislation on June 3 that contains certain proposed AI provisions prohibiting discrimination and requiring new AI Data Privacy Impact Statements/Evaluations. The American Privacy and Data Protection Act codifies across the United States that personal data cannot be collected, processed or transferred in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, gender, sexual orientation or disability, providing a federal privacy right against discrimination. Entities covered under the Act are required to undertake data evaluations to prevent data discrimination, including with respect to their AI training data or, for large data holders, their Data Privacy Impact Statements.

Areas of discriminatory concern highlighted in this new privacy legislation include AI targeting any individual under the age of 17 (a new age requirement); AI advertising for housing, education, employment, health care, insurance or credit opportunities; and AI determining access to, or restrictions on the use of, any place of public accommodation, particularly as such harms relate to the protected characteristics of an

Attorney Advertising

individual, including race, color, religion, national origin, gender, sexual orientation and disability. Although this bill was just recently introduced, AI businesses and users should follow its progress—despite the heavy congressional calendar, some are predicting it will move forward this year.

To provide a complete view of congressional intent on AI, we must mention the additional AI legislation pending before Congress regarding the federal agency use and misuse of AI, federal employee training on AI and federal government procurement practices regarding AI. Given the full legislative calendar and the limited number of active legislative days, it is unclear whether these bills will move forward.

The FTC Investigatory Focus on AI

In her June 16, 2022, Statement on Combatting Online Harms, Federal Trade Commission (FTC) Chairman Khan made clear that the FTC's investigatory focus on AI in order to prevent unlawful AI practices and abuses will move forward. Her statement emphasized that the FTC's increases in staff with technology expertise is primarily to handle such investigations. This focus was demonstrated in March 2022 in the FTC case against WW International, in which the FTC required the company to delete algorithmic data that was obtained illegally (in this case for children under the age of 13 without parental consent) and to destroy any algorithms through which the data was illegally harvested, in addition to fining the company $1.5 million. Implementing these sanctions to rebuild models and retrain an existing model with new data is not a simple task for any organization and would undermine the benefits of any AI used or offered in the marketplace.

This case comes on the heels of the December 2021 FTC Proposed Rulemaking to further regulate AI. The goal of this rulemaking is to establish guardrails around unfair and deceptive uses of personal data algorithms, in particular discriminatory outcomes. It is expected that this rulemaking will be put in place by the end of this year. This rulemaking follows the FTC's Artificial Intelligence "Do More Good Than Harm" guidance issued in April 2021. Given the FTC's regulatory scrutiny of AI, it is recommended that this guidance be integrated into each company's AI development, management and oversight processes, including starting with the right data sets, testing your results for discriminatory outcomes, and embracing data transparency and independent review.

State Legislative Artificial Intelligence Developments

Equally as active in this space are state legislators. Additional consumer privacy laws that will go into effect in 2023 in California, Colorado, Connecticut and Virginia include restrictions on profiling and automated decision-making as well as providing consumers with additional rights to delete and access data in AI. Notably, the consumer privacy law in Utah does not contain similar restrictions. If these privacy statutes apply to your business, whether you use or develop AI, planning how you will implement these obligations should be added to your company's operational road map today. We have highlighted a few of the critical concerns regarding profiling under the Virginia, Colorado and Connecticut statutes and under California's California Privacy Rights Act.

Under the Colorado, Connecticut and Virginia privacy laws, the right to opt out of profiling includes the right to opt out of processes that cause decisions that produce legal or similarly significant effects concerning a consumer. The definition of profiling is broadly and similarly defined in these statutes "as any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." While the phrase "legal and similarly significant effects" is not defined in Colorado's or Virginia's consumer privacy laws, Connecticut provides a definition that gives some clarity and could be harmonized across jurisdictions: "Decisions that produce legal or similarly significant effects concerning the consumer means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services."

For those companies and organizations falling under the jurisdiction of the CPRA, the law will bring employee and other personal data into the automated decision-making analysis, along with demanding transparency about AI logic. While the California Privacy Protection Agency (CPPA) has not yet issued them, the agency is charged with "[i]ssuing regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking [sic] technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking [sic] processes, as well as a description of the likely outcome of the process with respect to the consumer. These upcoming regulations are of great concern to AI developers and users alike. On May 4, 2022, the CPPA heard testimony for three hours from the AI community on the impacts of potential regulation on their businesses. The CPPA has not yet provided a timeline for when we will see these regulations, but current estimates suggest it will be at the end of this year at the earliest. The CPRA's regulations concerning the right to access regarding the logic transparency are being closely watched from an intellectual property perspective as well.

While we are waiting for state regulations to be issued in certain states, companies licensing or operating AI in these spaces should begin to consider how they can be transparent to consumers about their profiling practices and how to operationalize this profiling opt-out right and the other state law data subject access rights.

Current State Privacy-Adjacent AI laws and Proposed Legislation

States are increasingly enacting privacy- adjacent laws that impact AI, potentially creating another patchwork of compliance requirements for companies. These privacy-adjacent laws and proposed legislation fall within a few categories:

- Laws to review the adverse impact of artificial intelligence on state residents and businesses (Alabama, Illinois)
- Laws specifically prohibiting discrimination and unintentional bias with AI (Colorado and New Jersey, as well as New York City)
- Disclosure laws, such as those for California bots
- State agency AI procurement requirements

These laws and trends in legislation may evolve along with state consumer privacy laws, and should be considered as part of any company's AI compliance plan.

Protecting Business in the Face of Increasing AI Regulations

For users, purchasers, developers and managers of AI, we recommend the following best practices to stay in compliance with current laws and regulations impacting AI and to stay ahead of those to come:

- Understand how data is collected, used, processed and stored in all AI-powered technologies, and document these processes, including testing AI for potential discriminatory and bias outcomes, whether intended or not.
- Start the planning process now for implementing state consumer privacy (such as consumer profiling and access requests) and FTC requirements—be flexible to ensure your business can quickly pivot in the face of increasing regulation.
- Consider adopting a voluntary framework for all or part of your AI compliance activities. Several frameworks have been developed to aid companies using and building AI to adhere to "more good than harm" governance principles. Below are a few of the frameworks we've found of interest.

  Interactive Advertising Bureau's (IAB) Anti-Bias Framework. The IAB in November 2021 released a groundbreaking guide covering the subject of bias in the context of AI for marketing.

  NIST Framework. The National Institute of Standards and Technology (NIST) is developing a voluntary general framework to better manage risks to individuals, organizations and society associated with AI for businesses that operate AI and those that use these services. An initial draft of the NIST Framework was posted in March 2022.

  Singapore's AI Verify. In May 2022, the government of Singapore launched AI Verify, an AI Governance and Testing Framework and Toolkit, for companies that want to test their AI.

- Stay up to date on the quickly changing AI privacy regulatory and legislative landscape.

Related Professionals

Jessica B. Lee	jblee@loeb.com
Cathy Mulrow-Peattie	cmulrow@loeb.com

This is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This publication does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

7008 REV1 06-27-2022