Federal Guidance Hints at Robust Disclosure Requirements for use of Artificial Intelligence

Once a technology reserved for science fiction and fantasy, artificial intelligence (AI) now permeates almost every industry. In its most basic form, AI harnesses computer processing power, proprietary algorithms and large datasets to perceive and synthesize data in order to make decisions. The technology's applications are endless. AI is leveraged in facial recognition software, autonomous vehicles, credit card fraud detection and even video game development. Other applications may be less obvious but have more serious implications. AI-assisted automated decision-making software is used to make hiring decisions, approve loans, extend credit, administer social services, profile individuals in law enforcement contexts, predict recidivism rates and profile consumers.

Despite AI's influence in many sensitive areas such as housing, law enforcement, education and social services, many of the algorithms used to inform automated decision-making systems are proprietary. This means that both the public and regulators have a very limited understanding of how these systems work and what data is used to inform decisions. While protection for a developer's proprietary algorithms spurs innovation and generates profit, the "black box" nature of these systems presents a significant challenge to regulators faced with combating algorithmic bias, discrimination and error.

Current Patchwork of State Laws

California, Colorado (effective July 2023), Virginia and Connecticut (effective July 2023), have all passed legislation governing the use of AI. Only one state requires disclosures regarding how AI is used to make decisions. Specifically, California's CPRA charges the new California Privacy Protection Agency with adopting regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology," including public disclosure about the logic involved.

The remaining states provide opt-out rights, but regulations may add disclosure rights in the future. Colorado and Virginia will allow consumers to opt-out of "profiling" which is defined as "any form of automated processing performed on personal data" where such profiling is in furtherance of decision-making pertaining to housing, financial services, healthcare, criminal justice, employment and other sensitive areas. Similar to the GDPR's approach, Connecticut differs slightly by granting these opt-out rights only when decisions are made *solely* using automated processing.

Early Stages of U.S. Federal Regulation

In late 2022, the federal government turned its attention toward AI's role in making decisions, especially in more sensitive contexts where disparate impacts may arise. On August 22, 2022, the FTC published an Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security regarding Commercial Security (the ANPR) "to request public comment on the prevalence of commercial surveillance and data security practices that harm consumers." In October 2022, the White House released a Blueprint for an AI Bill of Rights (the Blueprint) "to help provide guidance whenever automated systems can meaningfully impact the public's rights, opportunities or access to critical needs."

Like California's CPRA, a primary focus in both the ANPR and Blueprint is the importance of transparency and disclosure. Citing the increased adoption of AI in decision-making models, the ANRP warns of new mechanisms for discrimination. The FTC posits whether new rules should require companies to disclose (1) data usage, (2) collection, retention, disclosure and transmission practices, (3) the use of automated decision-making systems to analyze or process data, (4) how they use data to make decisions and (5) their reliance on third-party decision-making tools, among other disclosures.

The Blueprint aligns with the ANRP's focus on transparency. One of the Blueprint's five core principles is "Notice and Explanation," which states that individuals should know when an automated system is being used to make decisions and how and why it contributes to outcomes that impact them. Both developers and deployers of AI systems should disclose "generally accessible plain language documentation including clear descriptions of the overall system functioning 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."

While notice, explanation and other disclosure requirements may offer some protection to consumers subject to automated decision-making, developers may be concerned that these requirements will put their proprietary information in jeopardy. While some large companies such as Amazon, Google and Meta, are beginning to embrace an opensource approach to AI development, many smaller companies still rely on the proprietary nature of their systems to generate profit and distinguish themselves in the market. Disclosure requirements, however, do not necessarily spell the end for this business model providing that companies plan carefully for how they will convey information to the public and regulators.

Preparing for Compliance

While a comprehensive AI regulatory framework is still likely a long way off, organizations that develop automated decision-making software should begin crafting statements now that (1) satisfy potential disclosure requirements suggested by both the ANRP and Blueprint and (2) offer sufficient protection for proprietary algorithms and related intellectual property. Additionally, companies that rely on service providers to process data using automated means will also likely have disclosure obligations stemming from a federal framework. These companies should reach out to their services providers now to request documentation regarding how data is processed and how AI impacts decision-making. Organizations that process data using AI technology may wish to consider the following compliance tips when crafting notice, use and other similar disclosures:

- Use plain language and avoid technical terms when describing automated systems. The disclosures must be easy to understand without a technical background.
- Any disclosure language should identify the entities responsible for designing, maintaining and using each component of the system.
- Notice language should be available prior to processing and updated regularly to account for any changes to the system.
- Keep explanations brief. To date, available guidance does not require a granular explanation that reveals proprietary information. While this may change, any publicly available explanations

should be drafted to protect sensitive and proprietary information. Focus on topics such as the quality of the datasets, accuracy of the model and the effects of the model on the public. Regulators are less concerned with how a model works and more concerned with who it impacts.

- Avoid charging the development team with drafting disclosure language. The development team should work closely with legal or compliance professionals to make sure any publicly available descriptions are easy to understand and devoid of sensitive or proprietary information.

Bond attorneys regularly assist and advise clients on an array of data privacy and intellectual property matters. If you have any questions about artificial intelligence, FTC compliance or IP-related issues, please contact Fred Price, Mario Ayoub or any attorney in Bond's intellectual property or cybersecurity and data privacy practices.