WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

U.S./EU Initiative Spotlights Cooperation, Differing Approaches to Regulation of Artificial Intelligence Systems

November 1, 2021

AUTHORS

Daniel K. Alvarez | **Laura E. Jehl** | **Kari Prochaska**

In late September 2021, representatives from the U.S. and the European Union met to coordinate objectives related to the U.S.-EU Trade and Technology Council, and high on the Council's agenda were the societal implications of the use of artificial intelligence systems and technologies ("AI Systems"). The Council's public statements on AI Systems affirmed its "willingness and intention to develop and implement trustworthy AI" and a "commitment to a human-centric approach that reinforces shared democratic values," while acknowledging concerns that authoritarian regimes may develop and use AI Systems to curtail human rights, suppress free speech, and enforce surveillance systems. Given the increasing focus on the development and use of AI Systems from both users and investors, it is becoming imperative for companies to track policy and regulatory developments regarding AI on both sides of the Atlantic.

EU-U.S. Shared Concern: Algorithmic Bias

At the heart of the debate over the appropriate regulatory strategy is a growing concern over algorithmic bias – the notion that the algorithm powering the AI Systems in question has bias "baked in" that will manifest in its results. Examples of this issue abound – job applicant systems favoring certain candidates over others, or facial recognition systems treating African Americans differently than Caucasians, etc. These concerns have been amplified over the last 18 months as social justice movements have highlighted the real-world implications of algorithmic bias.

U.S./EU Initiative Spotlights Cooperation, Differing Approaches to Regulation of Artificial Intelligence Systems

In response, some prominent tech industry players have posted position statements on their public-facing websites regarding their use of AI Systems and other machine learning practices. These statements typically address issues such as bias, fairness, and disparate impact stemming from the use of AI Systems, but often are not binding or enforceable in any way. As a result, these public statements have not quelled the debate around regulating AI Systems; rather, they highlight the disparate regulatory regimes and business needs that these companies must navigate.

EU Approach: Prescriptive Regulation

When the EU's General Data Protection Regulation ("GDPR") came into force in 2018, it provided prescriptive guidance regarding the treatment of automated decision-making practices or profiling. Specifically, Article 22 is generally understood to implicate technology involving AI Systems. Under that provision, EU data subjects have the right not to be subject to decisions based solely on automated processing (and without human intervention) which may produce legal effects for the individual. In addition to Article 22, data processing principles in the GDPR, such as data minimization and purpose limitation practices, are applicable to the expansive data collection practices inherent in many AI Systems.

Consistent with the approach enacted in GDPR, recently proposed EU legislation regarding AI Systems favors tasking businesses, rather than users, with compliance responsibilities. The EU's Artificial Intelligence Act (the "Draft AI Regulation"), released by the EU Commission in April 2021, would require companies (and users) who use AI Systems as part of their business practices in the EU to limit the harmful impact of AI. If enacted, the Draft AI Regulation would be one of the first legal frameworks for AI designed to "guarantee the safety and fundamental rights of people and businesses, while strengthening AI uptake, investment and innovation across the EU." The Draft AI Regulation adopts a risk-based approach, categorizing AI Systems as unacceptable risk, high risk, and minimal risk. Much of the focus and discussion with respect to the Draft AI Regulation has concerned (i) what types of AI Systems are considered high-risk, and (ii) the resulting obligations on such systems. Under the current version of the proposal, activities that would be considered "high-risk" include employee recruiting and credit scoring, and the obligations for high-risk AI Systems would include maintaining technical documentation and logs, establishing a risk management system and appropriate human oversight measures, and requiring incident reporting with respect to AI System malfunctioning.

While AI Systems have previously been subject to guidelines from governmental entities and industry groups, the Draft AI Regulation will be the most comprehensive AI Systems law in Europe, if not the world. In addition to the substantive requirements previewed above, it proposes establishing an EU AI board to facilitate implementation of the law, allowing Member State regulators to enforce the law, and authorizing fines up to 6% of a company's annual worldwide turnover. The draft law will likely be subject to a period of discussion and revision with the potential for a transition period, meaning that companies that do business in Europe or target EU data subjects will have a few years to prepare.

U.S./EU Initiative Spotlights Cooperation, Differing Approaches to Regulation of Artificial Intelligence Systems

U.S. Approach: Federal and State Patchwork

Unlike the EU, the U.S. lacks comprehensive federal privacy legislation and has no law or regulation as specifically tailored to AI activities. Enforcement of violations of privacy practices, including data collection and processing practices through AI Systems, primarily originates from Section 5 of the Federal Trade Commission ("FTC") Act, which prohibits unfair or deceptive acts or practices. In April 2020, the FTC issued guidance regarding the use of AI Systems designed to promote fairness and equity. Specifically, the guidance directed that the use of AI tools should be "transparent, explainable, fair, and empirically sound, while fostering accountability." The change in administration has not changed the FTC's focus on AI systems. First, public statements from then-FTC Acting Chair Rebecca Slaughter in February 2021 cited algorithms that result in bias or discrimination, or AI-generated consumer harms, as a key focus of the agency. Then, the FTC addressed potential bias in AI Systems on its website in April 2021 and signaled that unless businesses adopt a transparency approach, test for discriminatory outcomes, and are truthful about data use, FTC enforcement actions may result.

At the state level, recently enacted privacy laws in California, Colorado and Virginia will enable consumers in those states to opt-out of the use of their personal information in the context of "profiling," defined as a form of automated processing performed on personal information to evaluate, analyze, or predict aspects related to individuals. While AI Systems are not specifically addressed, the three new state laws require data controllers (or equivalent) to conduct data protection impact assessments to determine whether processing risks associated with profiling may result in unfair or disparate impact to consumers. In all three cases, yet-to-be promulgated implementing regulations may provide businesses (and consumers) with additional guidance regarding operationalizing automated decision-making requests up until the laws' effective dates (January 2023 for Virginia and California, July 2023 for Colorado).

Practical Implications for Businesses Leveraging AI Systems

Proliferating use of AI Systems has dramatically increased the scale, scope, and frequency of processing of personal information, which has led to an accompanying increase in regulatory scrutiny to ensure that harms to individuals are minimized. Businesses that utilize AI Systems should adopt a comprehensive governance approach to comply with both the complimentary and divergent aspects of the U.S. and EU approaches to the protection of individual rights. Although laws governing the use of AI Systems remain in flux on both sides of the Atlantic, businesses that utilize AI in their business practices should consider asking themselves the following questions:

1. Have we evaluated our AI systems for risk of harm to individuals, such as through a risk classification scheme or data protection impact assessments?

2. Do we maintain and update technical documentation to comprehensively describe the validation and testing of AI Systems?

3. Does our company evaluate and document opportunities for human intervention in its AI Systems processes?

4. Have we considered drafting public-facing statements, blog posts, or reports regarding our commitment to the transparent, fair, and ethical use of AI?

5. Does our company have an internal mechanism to comply with requests from individuals to opt-out of the use of their personal information in the use of AI Systems?

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez	**Laura E. Jehl**	**Kari Prochaska**
202 303 1125	202 303 1056	312 728 9080
dalvarez@willkie.com	ljehl@willkie.com	kprochaska@willkie.com