Supplement to the Los Angeles and San Francisco
Daily Journal
APRIL 17, 2019

TOP INTELLECTUAL PROPERTY LAWYERS

The data in the details: Issues to consider in AI

By Ken D. Kumayama and Shaya S. Afshar

An increasing number of businesses are turning to artificial intelligence and machine learning (AI/ML) to enhance their business models. AI/ML systems typically use massive datasets to "train" neural network computing systems, searching for patterns in data that are undetectable by humans, thereby improving algorithms' results. This article highlights several important topics that may be relevant to attorneys dealing with AI/ML technologies, whether for a client or employer.

Data Rights

When assessing the use of data in AI/ML systems, companies should consider how the data will be used and, with respect to third-party data, whether the company possesses the necessary intellectual property and contractual rights, especially since the data may be indefinitely retained in some form by AI/ML systems. Failure to secure sufficient rights could result in breach of contract, IP or privacy claims, and could also potentially call into question one's rights to both the AI/ML system and its results.

Contractual Data Rights. When data is used to train an AI/ML system, all users of the system benefit. Data from one customer may therefore benefit other customers, which may include competitors. Where training datasets include customer data, customer agreements should include sufficiently broad data rights to permit their use in AI/ML systems. While language such as "customer data may be used to improve the services and related technologies" may be sufficient, agreements should be reviewed on a case-by-case basis.

Web Scraping. Data scraping, or harvesting data from third-party websites for commercial purposes, poses its own risks. While the jurisprudence continues to evolve, website owners opposing this practice have brought numerous claims, including breach of contract, IP infringement, trespass to chattels, and violations of the Digital Millennium Copyright Act and Computer Fraud and Abuse Act. Companies should therefore proceed carefully before using scraped data to train AI/ML systems.

Data Privacy

While the European Union's General Data Protection Regulation (GDPR) has garnered the most attention, an increasing number of jurisdictions have enacted data privacy laws that regulate the processing (e.g., collection, storage, use, transfer, modification) of personal data. In the U.S., the California Consumer Privacy Act is slated to take effect in January 2020. Companies that use personal data with AI/ML systems should be mindful of these regulations.

Anonymization. As a threshold matter, data that is "anonymized" is not subject to GDPR or other privacy laws. However, the threshold to establish anonymization under GDPR is high. Businesses should carefully consider whether they meet this test, as pseudonymization — a technical measure to reduce security risks associated with processing personal data — may not remove the data from GDPR's purview. Where the data may be re-identified by combining it with other data held by the organization or that is publicly available, it will not satisfy the requirements of anonymization and will therefore remain subject to privacy regulation.

Consent. While data privacy laws generally permit a data subject's informed consent to be a lawful basis for processing personal data, this approach may not be ideal for AI/ML systems. Data subjects can revoke their consent at any time under GDPR and can request that their data be deleted. Practitioners should consider whether obtaining consent to use personal data "internally to improve services" will suffice or if more granularity or affirmative steps may be required.

Data Minimization. The GDPR principle of data minimization mandates that personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Since businesses working to improve AI/ML systems tend to indefinitely retain training data, organizations should carefully consider whether retention periods for training data is possible, and, if not, have deletion processes in place. Holding more data than necessary can create additional liability for businesses.

Automated Decision Making (ADM). Data privacy laws may have specific prohibitions or requirements that impact the use of personal data for AI/ML systems. For example, Article 22 of GDPR, which regulates the use of profiling to evaluate certain personal aspects of data subjects (e.g., personal preferences, health, location) restricts decisions "based solely on automated processing" and automated individual decision-making. Companies using AI/ML systems should consider if their use of personal data violates this restriction. Relatedly, Washington State introduced a bill in early 2019 aimed at eliminating bias and ensuring transparency regarding the use of automated systems by the government.

National Security/Export Regulations

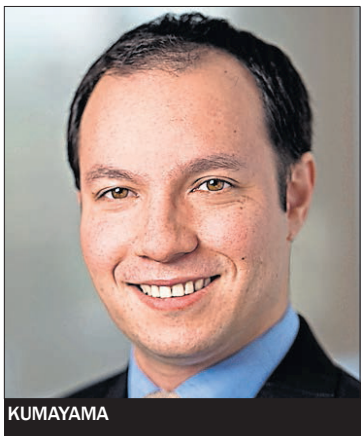
Governments have passed various laws to enhance their standing as leaders in AI/ML technology or otherwise further their national security goals. Such laws may have far-reaching effects on how companies do business in these jurisdictions, including China, Russia and the U.S.

Data Localization. China and Russia have both passed laws requiring personal data to be processed in-country. Organizations doing business in these countries should consider where and how to store the personal data received from these countries, and whether such data may be used as training data for AI/ML systems.

CFIUS/FIRRMA. In November 2018, the U.S. government proposed to treat AI/ML technology as an "emerging technology" critical to U.S. national security. As a result, AI/ML technology in some form is likely to become export-controlled in the near future and licenses likely will be required for certain countries (and for the release of such technology to nationals of these countries, even in the United States). Once designated as an emerging technology, AI/ML technology also will be treated as a critical technology for purposes of the newly enacted Foreign Investment Risk Review Modernization Act (FIRRMA). Under FIRRMA, transactions involving foreign persons that touch on U.S. critical technology are subjected to heightened scrutiny and may trigger a requirement to make a submission to the Committee on Foreign Investment in the United States (CFIUS). In light of FIRRMA, there is greater risk that CFIUS will more heavily condition or outright block acquisitions of, and certain noncontrolling investments in, U.S. companies with advanced AI/ML technologies.

As AI/ML technologies play an increasingly important role in society, the legal issues will only increase in number and complexity, challenging attorneys to stay abreast of the ever-changing legal landscape.

Ken D. Kumayama, *left, is a counsel and* **Shaya S. Afshar** *is an associate in the Intellectual Property and Technology Group in the Palo Alto office of Skadden, Arps.*


KUMAYAMA


AFSHAR