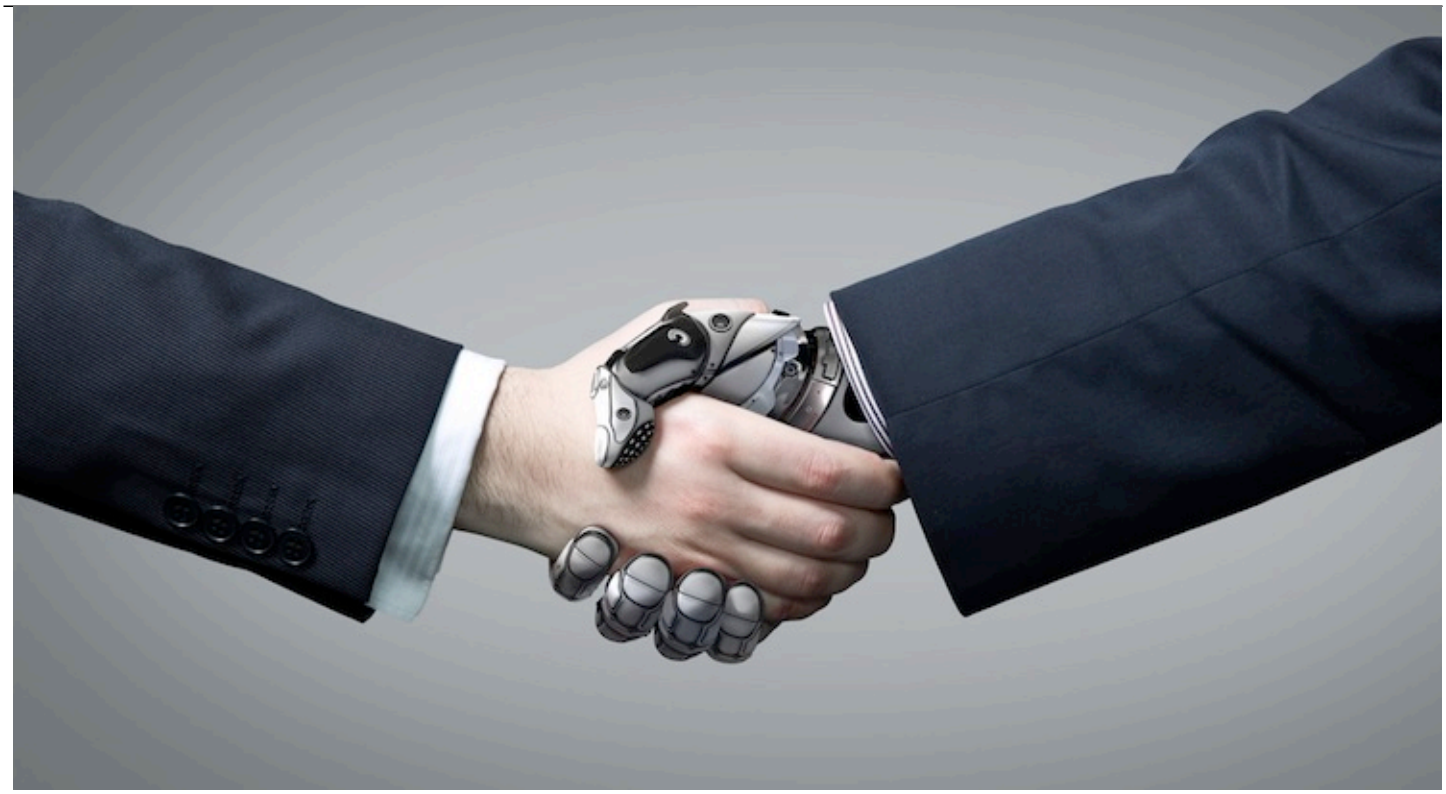
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Next Frontier: A Legal Forecast for the Age of Artificial Intelligence

Intellectual Property

Technology, Privacy, and eCommerce



Merely twenty years ago, artificial intelligence (AI) was the plot line in movies, books, and short stories. While it loomed on the horizon, it is only now getting the attention of world, and business leaders. A few days into 2016, Mark Zuckerberg of Facebook announced that he plans to spend 2016 developing an AI system to help run his life. He stated in his Facebook post: “My personal challenge for 2016 is to build a simple AI to run my home and help me with my work. You can think of it kind of like Jarvis in Iron Man.” He continued by outlining his approach: “I'm going to start by exploring what technology is already out there. Then I'll start teaching it to understand my voice to control everything in our home — music, lights, temperature and so on.” Zuckerberg also discussed the practical applications for the AI, from a facial-recognition doorbell system, to a baby monitor for his new child. He also plans to merge AI with virtual reality, visualizing “data in VR” to better analyze his services and organizations.

As the topic is becoming top of mind, the Wikimedia Foundation recently hosted an “Artificial Intelligence and the Law” panel in San Francisco to discuss the legal challenges and solutions presented by AI, ranging from lethal autonomous weapons, driverless cars, and ROSS, the first robot attorney. The panel featured impressive names such as Rebecca Crootof, executive director of the Information Society Project at Yale Law School; Jimoh Ovbiagele, co-founder and CTO at ROSS Intelligence; Christopher Reed, COO and general counsel at Zenti; David Ahn, Partner at Fenwick & West LLP; and moderator Chuck Roslof, legal counsel at Wikimedia. The panelists identified a few of the prominent legal and ethical issues surrounding AI that will arise over the coming years.

The uses and limits of analogy

Crootof spoke about the benefits and drawbacks associated with using analogies to discuss new technology. Analogies make new technologies accessible and provide a framework for thinking about

them — but they also box us in. Crootof noted that autonomous weapon systems are usually thought of as Terminators or more independent drones, but animals might be the better analogy. And all three options — combatants, weapons, and animals — constrain us from thinking about unembodied autonomous cyberweapons. She also noted how thinking of autonomous vehicles as “self-driving cars” limits our imagination with respect to how they might be designed, used, and regulated.

Appropriate level of human control

According to Crootof, “AI challenges assumptions that we used to take for granted — namely, the necessity of human decision making.” She listed various questions raised by introducing AI into weapon systems, including: What constitutes meaningful human control over an attack? Does one have to pull a trigger to exercise control? Is simply having a human observer with veto power sufficient? Or is it enough that human beings wrote the original code? Who should be held accountable when an autonomous weapon system commits a war crime? All of these questions require us to determine the appropriate amount of human control over AI — and who should be held responsible when their unpredictable actions cause harm.

EU’s AI “explainability” requirement

EU lawmakers are contemplating an “explainability” requirement for AI, requiring any significant decision made via AI software be “explainable.” For example, if AI makes a decision to categorize a person, the decision must be explained in a way humans can understand. Reed opposed such a requirement, saying, “Fundamentally, people are legislating about something they have no clue about. They unrealistically assume that for AI to be accountable there has to be a link to a causality that a person understands.” He added, “It will be hard for the European Union to enforce this legislation because it may be hard to discern the effects of AI.” Ovbiagele shared similar sentiments, saying, “Much of AI cannot be explained. It is often hard to explain how AI reaches decisions. In fact, humans can’t always explain how they make decisions. So this requirement may be fundamentally flawed.”

Intellectual property

Like most technology, AI is primarily protected by patents, copyrights, and trade secrets. “Patents provide the strongest protection” for AI, said Ahn. He explained that because AI is primarily technically driven, “AI inventions are mostly patentable, although some inventions on abstract AI concepts may be problematic in view of recent court decisions.” However, an issue arises when AI systems create works such as writing or music. Are these works protectable? “The answer to this question at this time is ‘no,’” Ahn explained. IP laws are aimed at natural persons. So accordingly, “at this time, it’s highly unlikely that an AI would be recognized as an inventor, author or creator.”

Data and privacy

Reed suggested that perhaps we need to reframe the debate over AI and privacy issues. “We have to accept that AI will bring both good and bad. And we can’t get permission for everything,” he said. Instead of rejecting AI outright, policy makers should seek alternative solutions. For example, “some suggest that [AI] that take information should be in a special category, like common carriers, and held to a higher standard,” Reed said. Another issue is that AI data sets can contain personal information, which may lead to privacy concerns. “We get this question a lot. Privacy issues in ROSS are not unique. Data has been collected over decades,” Ovbiagele asserted. He explained, “Machine

learning was created to address massive amounts of data. We are not collecting more data because of machine learning. We are using machine learning because we have massive data." Using this argument, he concluded that AI will not create new potential privacy violations beyond those that are already present in the existence of mass data. Crootof, however, challenged this view by pointing out that the use of more powerful tools (i.e. machine learning) may amplify the potential damage of these privacy violations. "I'm comforted by the idea that my data is a needle in a very large haystack," she observed. "But if you have a powerful magnet, my data isn't nearly as safe."

While the panelists raised critical issues, there is an opposing concern that we are overreacting, over-regulating, and unwittingly chilling innovation. Ultimately, anyone can use the same powerful tools for good or evil. No amount of regulation can fully prevent misuse or abuse of a particular tool. For example, a knife can be used to cook a family dinner, but in the wrong hands, to kill another person. Understanding the tool's intent and training the user matter. We cannot simply blame technology for human mistakes and misuse. In this crucial development period, we must balance our urge to regulate with the need to innovate, and recognize that there is no substitute for humanity.

Olga V. Mack

Fellow

CodeX

Olga V. Mack is a fellow at CodeX, The Stanford Center for Legal Informatics, and a Generative AI Editor at law.MIT. Mack shares her views in her columns on ACC Docket, Newsweek, Bloomberg, VentureBeat, Above the Law, and many other publications.

Mack is also an award-winning (such as the prestigious ACC 2018 Top 10 30-Somethings and ABA 2022 Women of Legal Tech) general counsel, operations professional, startup advisor, public speaker, adjunct professor, and entrepreneur. She co-founded SunLaw, an organization dedicated to preparing women in-house attorneys to become general counsels and legal leaders, and WISE to help female law firm partners become rainmakers.

She has authored numerous books, including Get on Board: Earning Your Ticket to a Corporate Board Seat, Fundamentals of Smart Contract Security and Blockchain Value: Transforming Business Models, Society, and Communities. She is working on her next books: Visual IQ for Lawyers (ABA 2024), The Rise of Product Lawyers: An Analytical Framework to Systematically Advise Your Clients Throughout the Product Lifecycle (Globe Law and Business 2024), and Legal Operations in the Age of AI and Data (Globe Law and Business 2024).

Katia Bloom

Commercial Lawyer and Associate General Counsel

ForgeRock

Katia Bloom is a fast-paced and strategic commercial lawyer. Currently, she is the associate general counsel at ForgeRock. Previously, she headed up legal for Avira, Inc., was a founding partner at E Squared Law Group, advising many start-up clients and was in-house counsel at Anesiva. She is actively involved in the Association of Corporate Counsel and a number of organizations promoting

women in the legal profession.