2021

The Law of AI

Margot Kaminski
University of Colorado Law School

The Law of AI

Author : Margot Kaminski

Date : October 25, 2021

Michael Veale and Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act* 22(4) **Computer L. Rev. Int'l** 97-112 (2021).

The question of whether new technology requires new law is central to the field of law and technology. From Frank Easterbrook's "law of the horse" to Ryan Calo's law of robotics, scholars have debated the what, why, and how of technological, social, and legal co-development and construction. Given how rarely lawmakers create new legal regimes around a particular technology, the EU's proposed "AI Act" (Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts) should put tech-law scholars on high alert. Leaked early this spring and officially released in April 2021, the AI Act aims to establish a comprehensive European approach to AI risk-management and compliance, including bans on some AI systems.

In *Demystifying the Draft EU Artificial Intelligence Act*, Michael Veale and Frederik Zuiderveen Borgesius provide a helpful and evenhanded entrée into this "world-first attempt at horizontal regulation of AI systems." One the one hand, they admire the Act's "sensible" aspects, including its risk-based approach, prohibitions of certain systems, and attempts at establishing public transparency. On the other, they note its "severe weaknesses" including its reliance on "1980s product safety regulation" and "standardisation bodies with no fundamental rights experience.". For U.S. (and EU!) readers looking for a thoughtful overview and contextualization of a complex and somewhat inscrutable new legal system, this Article brings much to the table at a relatively concise length.

As an initial matter, it's important to understand that the Draft AI Act is just the beginning of the European legislative process. Much can still change. And the Act must be understood in legal context: it is entwined with other EU Regulations (such as the GDPR), Directives (such as the Law Enforcement Directive and Unfair Commercial Practices Directive), and AI-specific initiatives in progress (such as the draft Data Governance Act and forthcoming product liability revisions).

The AI Act itself focuses on risk management and compliance, looking at threats to physical safety and fundamental rights. At its core, the Act is an attempt to reduce trade barriers while also addressing fundamental rights concerns. According to Veale and Borgesius, by primarily relying on product safety regulations and bodies, the AI Act gets the balance wrong.

Not all is bad, however. Veale and Borgesius appreciate the AI Act's division of AI practices into four risk levels: unacceptable (Title II), high (Title III), limited (Title IV), and minimal (Title IX). AI systems with unacceptable risks trigger full or partial prohibitions, while high risk systems are regulated based on the EU approach to products safety (the New Legislative Framework or NLF). But Veale and Borgesius note that at closer examination, neither the prohibitions nor the regulations are as robust as they might appear.

For example, take the ban on biometric systems, which at first appears to be precisely what some scholars have called for. The Act bans most "real-time" and "remote" law enforcement uses of biometric systems in publicly accessible spaces (Art. 5(1)(d)). Notably, systems that analyze footage after-the-fact are not included. Nor is live biometric identification online, nor is the use of remote biometric identification for non-law enforcement purposes, which falls under the GDPR. And Member States may create yet more exceptions, by authorizing certain law enforcement uses of real-time biometrics, so long as they include certain safeguards. Veale and Borgesius rightly point out that the ample

exceptions to the Act's limited biometrics ban mean that the infrastructure for biometrics systems will still be installed, leading some to claim that the Act "legitimises rather than prohibits population-scale surveillance." Moreover, nothing in the Act prevents EU companies from marketing such biometrics systems to oppressive regimes abroad.

The most complex and unfamiliar aspect of the Act is its regulation of high-risk systems. There, according to Veale and Borgesius, the Act collapses the protection of fundamental rights into the EU's approach to product safety, to its detriment. The NLF is used to regulate toys, elevators, and personal protective equipment, and is completely unfamiliar to most information law scholars (we will have to learn fast!). Under the NLF, manufacturers perform a "conformity assessment" and effectively self-certify that they are in compliance with "essential requirements" under the law. Here, those requirements are listed in Chapter 2 of the Act, and include a quality management system, a risk management system, and data quality criteria, among other things. Manufacturers can mark conforming products with "CE," which guarantees freedom of movement within the EU.

By contrast, Veale and Borgesius point to the path not taken: EU pharmaceutical regulation requires pre-marketing assessment and licensing by a public authority. Here, the public sector has a much more limited role to play. There are "almost no situations" in which such industry AI self-assessments will require approval by an independent technical organization, and even then, such organizations are usually private sector certification firms accredited by Member States.

Post-marketing, the AI Act again reflects the NLF by giving "market surveillance authorities" (MSAs)—typically existing regulatory agencies—the power to obtain information, apply penalties, withdraw products, etc. While AI providers must inform MSAs if their own post-market monitoring reveals risks, Member States have discretion as to which authorities will be responsible for monitoring and enforcing against standalone high-risk AI systems. In practice, Veale and Borgesius observe that this will put technocratic government agencies ordinarily concerned with product regulation in charge of a range of tasks well outside their usual purview: "to look for synthetic content on social networks, assess manipulative digital practices of any professional user, and scrutinise the functioning of the digital welfare state…[t]his is *far* from product regulation."

Moreover, Veale and Borgesius point out that private standards-setting organizations will determine much of the content of the law in practice. The European Commission will likely mandate that several European Standardisation Organizations develop harmonized standards relating to the Act that companies can follow to be in compliance with it. For internet governance buffs, the problems with deciding on fundamental values through privatized processes are familiar, even old hat. But as Veale and Borgesius observe, the Act's "incorporation of broad fundamental rights topics into the NLF [regime]… spotlight[s] this tension of legitimacy" in the EU products safety context.

This Article contains many additionally helpful sections, including a summary of the Act's transparency provisions, approach to human oversight, and the potential confusion around and problems with the scope of the Act's harmonization efforts. I do wish the authors had spent more time on the lack of rights, protections, and complaint mechanisms for what they call "AI-systems-subjects"—the individuals and communities impacted by the use of AI. As Veale and Borgesius observe, neither the standards-setting organizations nor the relevant government bodies are required to take input or complaints from impacted persons. They characterize this primarily as bad regulatory design, noting that "the Draft AI Act lacks a bottom-up force to hold regulators to account for weak enforcement." To those of us steeped in the GDPR's emphasis on individual rights, the absence of individual rights here is more shocking. I would be curious to learn about whether this choice/oversight is a real problem, or whether other EU laws nonetheless enable affected individuals to participate in the EU governance of AI.

Overall, this article is a much-needed guide to an immensely significant regulatory effort. For scholars, it raises complex questions about not just when new technology leads to new law, but how the choice of legal regime (here, product safety) establishes path dependencies that construct a technology in particular ways. Veale and Borgesius are to be applauded for their noted expertise in this space, and for doing the work to make this this regime more accessible to all.

Cite as: Margot Kaminski, *The Law of AI*, JOTWELL (October 25, 2021) (reviewing Michael Veale and Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act* 22(4) **Computer L. Rev. Int'l** 97-112 (2021)), https://cyber.jotwell.com/the-law-of-ai/.