

DESPITE LACK OF DIRECT REGULATION, AI IS NO LONGER THE ‘WILD WEST’

A Morrison & Foerster webinar examined the pressure that privacy laws such as the GDPR are already putting on companies to be transparent in their use of AI.

BY FRANK READY

To see or not to see—that is the question. Or at least it was the one at the heart of Wednesday’s “Privacy Issues in AI: What Companies Need To Know Before Deploying AI” webinar hosted by law firm Morrison & Foerster.

And one of the first things the companies need to know is the difference between a “black box” or a “white box” artificial intelligence (AI) system. While the former is generally opaque in its reasoning, a white box solution is typically more transparent, allowing humans to see the process by which it arrived at a result.

Panelist Marijn Storm, an associate with Morrison & Foerster, noted that this is



Credit: peshkov/stock.adobe.com

important because AI often can’t tell the difference between correlation and causation. In other words, it’s good at drawing connections between data, but may ultimately misinterpret why that connection exists—which can lead to bias absent an opportunity for human review.

“There are also correlations in there that as humans we would say ‘well that happened by chance’ because they have nothing to do with one another,” Storm said.

Such insights can be vital because while there may not be too many laws specifically targeting AI on the books,

organizations could still run afoul of any number of other applicable regulations. Panelist Cecillia Xie, an associate at Morrison & Foerster, said that existing privacy laws such as the EU's General Data Protection Regulation (GDPR) already place boundaries around many aspects of AI, even if artificial intelligence isn't specifically called out by name.

"The use of AI really isn't as much of a wild, wild west as one might think because there are privacy laws that have overlap with the use of AI. In the U.S., there's consumer privacy laws, anti-discrimination laws and other consumer protection laws," Xie said.

The common theme among many of those different laws

or regulations is transparency and explainability. In other words, companies should be able to explain how an AI generated an outcome in plain English, as well as notify consumers, job applicants or employees how their data will be used by such a tool.

Xie used the example of a job candidate who is asked to provide data around their ethnic origin that will eventually be fed into an AI system. "Potentially the way in which ethnic origin [data] might be used could be surprising to me, in which case you might want to consider principles of transparency and notice," she said.

Even with all of the appropriate notices in place,

companies may still want to be wary about when and where they use AI, especially if the decisions being rendered are tied to hiring decisions or workplace opportunities.

Panelist Christine Lyon, a partner at Morrison & Foerster, noted that organizations are ultimately responsible for any decision that's reached using a piece of AI software, even if the technology in question came from a third party provider.

"The algorithm made you do it' really isn't going to be a suitable defense," Lyon added.

Frank Ready is a reporter on the tech desk at ALM Media. He can be reached at freedy@alm.com