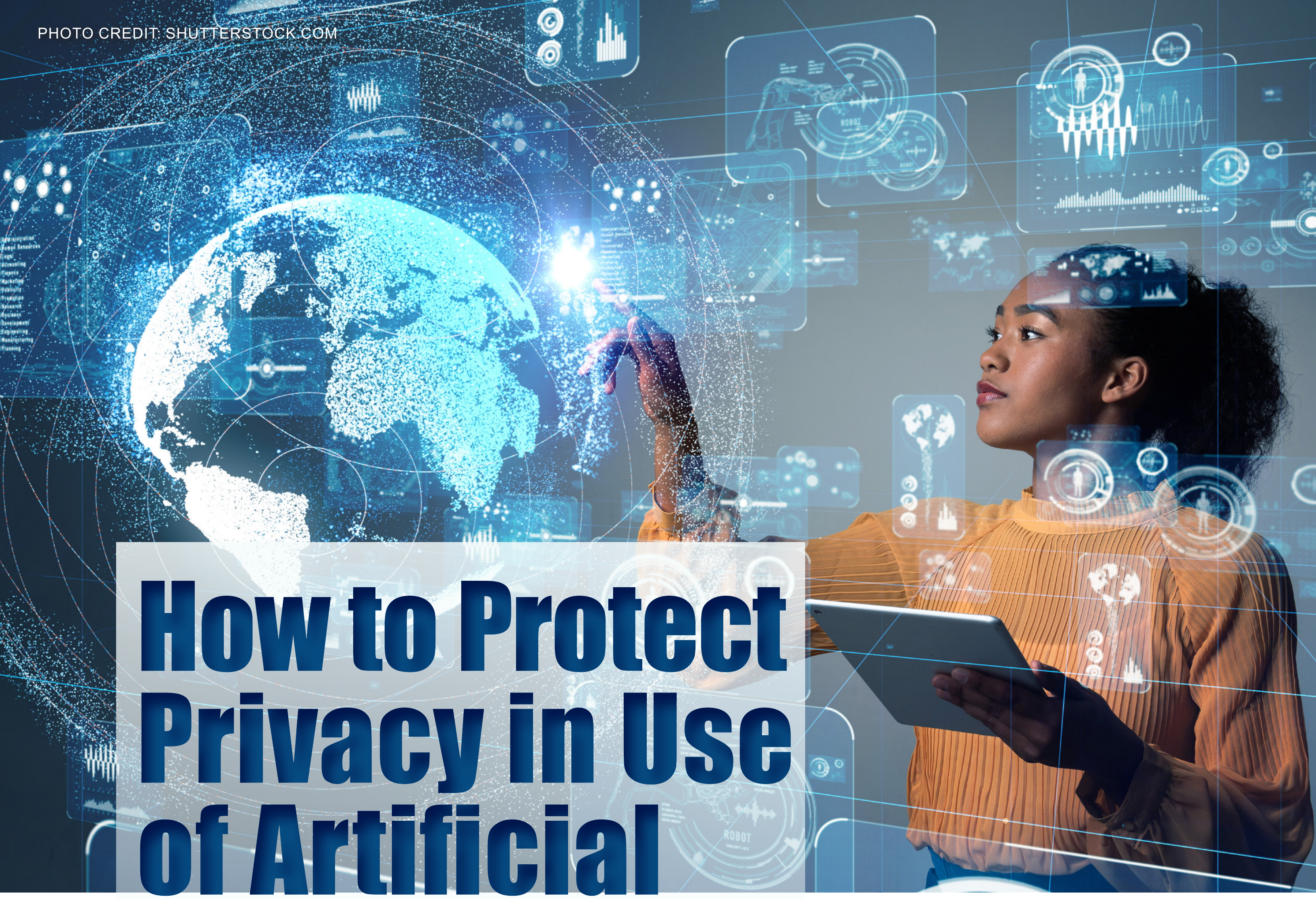
PHOTO CREDIT: SHUTTERSTOCK.COM



How to Protect Privacy in Use of Artificial Intelligence

BY JESSICA E. BROWN, ESQ.

The rise of artificial intelligence (AI) has brought to the forefront new ethical considerations, including how personal data is handled. Already, Article 22 of the European Union (EU)'s General Data Protection Regulation governs automated decision-making, requiring companies to provide notice where automated decisions are made and provide human review of any such decision. Unlike traditional retail or gaming industries, AI offerings cross borders, which means companies must think about and comply with laws where the AI is used, not just where it is developed.

A mooted federal privacy law, the American Data Privacy and Protection Act, would require large data holders to conduct algorithm impact assessments where there is a risk of harm to an individual or group when processing personal data. Privacy is further implicated by generative AI, which uses neural networks to identify patterns and structures within existing data to generate new and original content.

The Federal Trade Commission is investigating OpenAI, one of the leading providers of large language models, about concerns that ChatGPT can publish false information about individuals. Privacy regulators across Europe and Canada have expressed concern about the use of personal data to train large language models as well as individuals' ability to block usage of their data for this purpose. A suit is pending in California requesting compensation for the scraping of personal data to train generative AI engines. On the regulatory front, the EU is contemplating an AI Act that would govern development and use of AI systems from conception to going to market. In the U.S., the White House and other federal agencies are looking at an overall national AI strategy and AI governance more generally. And states and localities are also considering and enacting measures. Like any technology, as AI grows in importance and has more of an impact on our lives, governments will want to make sure companies are thinking about the risks of the

CONTINUED ON PAGE 17

CONTINUED FROM PAGE 15

How to Protect Privacy in Use of Artificial Intelligence

technology as well as its benefits, and how to address those.

These issues are pertinent not just for developers of AI offerings, generative or otherwise, but for any company that uses AI, whether internally or to provide services to customers. And, more broadly, AI implicates a host of ethical considerations in how it interacts with individuals. To navigate these waters, companies need to keep some key principles at the forefront. After all, people use technology they trust, and for a technology powered by data like AI, people will only share their personal data if they are sure it is protected. That means not using more data than needed, providing proper security, letting people know how their data will be used, and providing appropriate individual rights.

Privacy is about enhancing trust and giving people comfort that their data will be used responsibly and in a way that benefits them. While Nevada has some privacy laws covering data brokers and, most recently, use of health data, it does not yet have a comprehensive privacy law. While this lack of regulation may be seen by some as a benefit, as it creates flexibility, it also poses risks, as people may be less willing to share data in the absence of protections. As data is what powers AI, this could impede AI development within Nevada. And because of the cost of developing AI offerings, especially generative AI, Nevada companies will want to sell those across the U.S. and globally, meaning they will have to comply with existing legal regimes elsewhere. But even in the absence of regulation, companies can take steps to build trust.

One element in building trust is transparency, both to customers and end users, so they know they are interacting with an AI system and have some insight into how it operates. Another is understanding what data goes into the system – where it comes from, what rights attach to it, and how the system uses it. Where possible, companies should protect privacy by de-identifying data. There are techniques like tokenization that can de-identify data, passing on essential attributes while shielding the identity of the individuals to reduce risk of data loss or breach. Identities can be re-associated when the content generated by the large language model returns. And, of course, remember that these large language models are offered by third parties, so companies should make sure that have the right contractual terms in place and are comfortable with their privacy programs and controls.

Speaking of the data used, data is at the heart of AI technology. More specifically, data quality is essential to high-value outputs. Companies using AI systems must think about the source of the data used to power the system – is the data "clean" and free of errors? Equally important is representativeness: the data used to develop the AI system needs to reflect the communities that will be impacted by it, to ensure it operates as intended. And taking steps to address potential bias is vital, as algorithmic bias is a concern, even recognizing that humans are biased as well, as all of us bring our impressions and unconscious biases with us. To minimize unwanted bias, it is important to make sure that protected characteristics are not part of the data the AI system acts upon. Then, where appropriate, companies should do bias studies to test whether the algorithm exhibits bias in some way and then make adjustments as needed. While Elon Musk has set the goal of his new venture xAI to be "maximum truth-seeking AI," the fact remains that bias in both data and humans exists and must be controlled for in AI development. Because it is the right thing to do, and because not doing so would open companies up to tort liability and anti-discrimination laws like Title VII of the Civil Rights Act in the case of employment discrimination.

The best way to address all of these items is to have a strong AI governance program that takes these items into account at the start and makes sure they are thought about and addressed. By thinking about what problem the system is trying to solve, the data that is used to derive insights, and how those insights will be used, companies can consider risk at every step in the process from conceptualization to development to deployment to usage and take steps to mitigate them. With governance that embodies transparency, privacy, ethical design, and human oversight, AI's full potential can be realized in a way that benefits all.

JESSICA E. BROWN is a deputy attorney general for the state of Nevada, and a former technologist and developer.