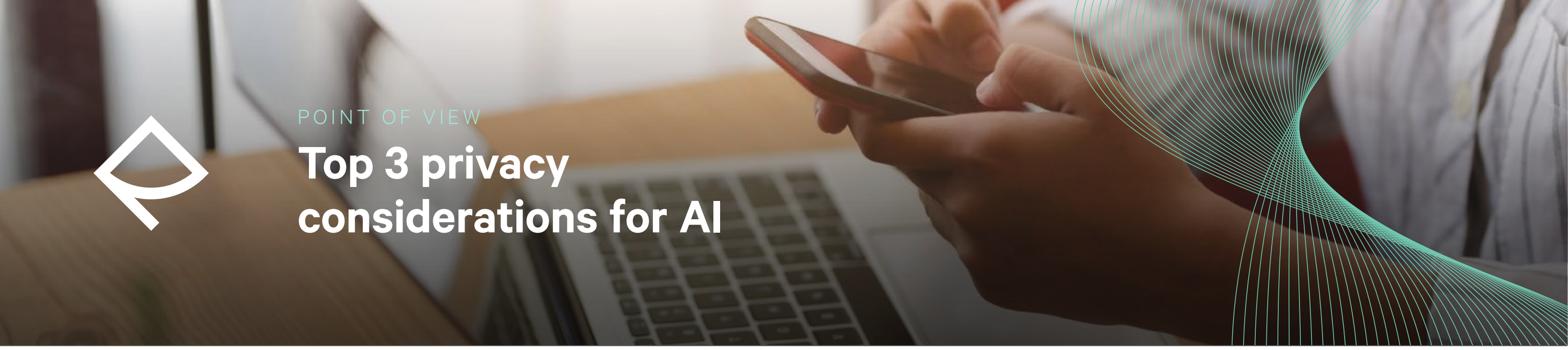

POINT OF VIEW

Top 3 privacy considerations for AI

Jose Araujo
Senior Manager,
Strategy

June 2, 2020

Decades ago, the term “artificial intelligence (AI)” made us think about robots roaming planet Earth—computers capable of thinking, feeling, and doing autonomously. The technology promised to revolutionize humankind, and while it hasn’t yet managed to meet those expectations, it has started to reshape our healthcare landscape.

Technological advances in AI are continuously being applied to new areas within the healthcare industry. AI allows for faster, more accurate, and more personalized healthcare delivery than ever before. As marketing becomes increasingly data driven, more pharmaceutical companies and healthcare brands may be compelled to introduce AI to power initiatives like CRM, media deployment, and creative personalization. **As a marketing tool, AI helps us unlock opportunities to engage with patients or healthcare professionals in a more personalized way, ensuring a better user experience throughout the journey.**

However, as is always the case with any new technology, there are considerations to be aware of before implementing, particularly when it comes to data privacy. We used to only worry about HIPAA regulations, but now, we also must consider the implications of the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This expanding regulatory and data privacy landscape poses a unique challenge to AI technologies that rely so heavily on user data.

How can you have the best of both worlds: the power and personalization of AI tools, while staying ahead of the data privacy regulations?

At Evoke, we rely on AI to deploy customized CRM programs and power our Customer Experience (CX) suite of offerings, so we know the best way to move forward, while protecting your brand and your customers. We always tell clients to keep 3 things in mind:

1. Start with a security audit

With a slew of new companies working in the AI landscape, it is easy to get excited about new products and offerings. It is now possible to fully automate your end-to-end marketing funnel by leveraging third-party technology. However, for each AI investment you make, you’re turning over company and customer data to power the technology. It is important to be extra vigilant to ensure any third-party technology providers go above and beyond to protect sensitive user data.

Specifically, we recommend undergoing a thorough security audit with any new technology vendors who may be handling sensitive data to ensure they are not only HIPAA compliant, but also compliant with GDPR and CCPA and in a position to quickly adapt according to any new regulation coming down the pipeline or other external threats. Think of a data security audit like a home inspection. You would never purchase a new house without a thorough inspection of the most important elements. A data security audit provides the same peace of mind and can help avoid disasters down the line.

Our Evoke Technology and CX teams can be equal partners to guide you through the evaluation and security audit process of any new third-party vendors to ensure data are secure and privacy is handled with the highest standards.

2. Diversify your data sets

At Evoke, when we think of the data needed to power AI technology, we always stress the **3 Vs: volume, variety, and velocity.**

Volume
Use a large volume of data to better machine learning and unbiased decision making.

Variety
Input a variety of data to help broaden the consideration set.

Velocity
Pay attention to the velocity of data (AI only moves as fast as your slowest piece of data).

AI technology cannot be overly reliant on a single source of data that may, at some point, be jeopardized by regulations or user limitations. At the setup stages of any new campaign or any new AI vendor, **when defining your data streams for your most important indicators, it is important to understand the sources of your data and how privacy is weaved into some of the more crucial elements of data collection**. To borrow another analogy, think of this like building a stock portfolio. Putting all your investments in a single stock means your entire portfolio is at risk if something were to happen to that one company. Just like portfolio diversification can protect you in a changing market, diversifying your data sources ensures your AI capabilities are more resilient to any changes down the line.

If you lack the data volume or variety necessary to power a truly effective AI technology, there are options available to diversify your data sets to ensure your AI engines are more adaptable to future changes in data privacy regulations.

3. Future-proof your investment

The AI regulation infrastructure is changing quickly. GDPR and CCPA are likely only the beginning of data privacy regulations that are likely to be developed as government plays catch-up to protect user privacy. Therefore, it is imperative to invest in a technology infrastructure that is nimble enough to quickly adapt to any changes—regulatory or otherwise.

Leveraging cloud-based AI infrastructure and providers ensures easier pivots to any data requirement changes down the line. These adaptable foundations will be crucial in being able to continue taking advantage of AI technology in a compliant manner and benefit from its capabilities.

If you're unsure how to construct the best AI infrastructure to keep up with the evolving times, our Evoke Technology and CX teams can help you construct an AI technology architecture so you're investing in a system that can stand the test of time.

The Evoke Artificial Intelligence Center of Excellence helps pharmaceutical and health and wellness clients navigate an ever-changing landscape of new technology partners and regulatory changes. Our practices and partner assessment processes are designed with patient privacy at the forefront to ensure we can deliver best-in-class personalized experiences while complying with data regulations. To request more information, contact business@evokegroup.com.