ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

No, Every Company Doesn’t Need an AI Policy

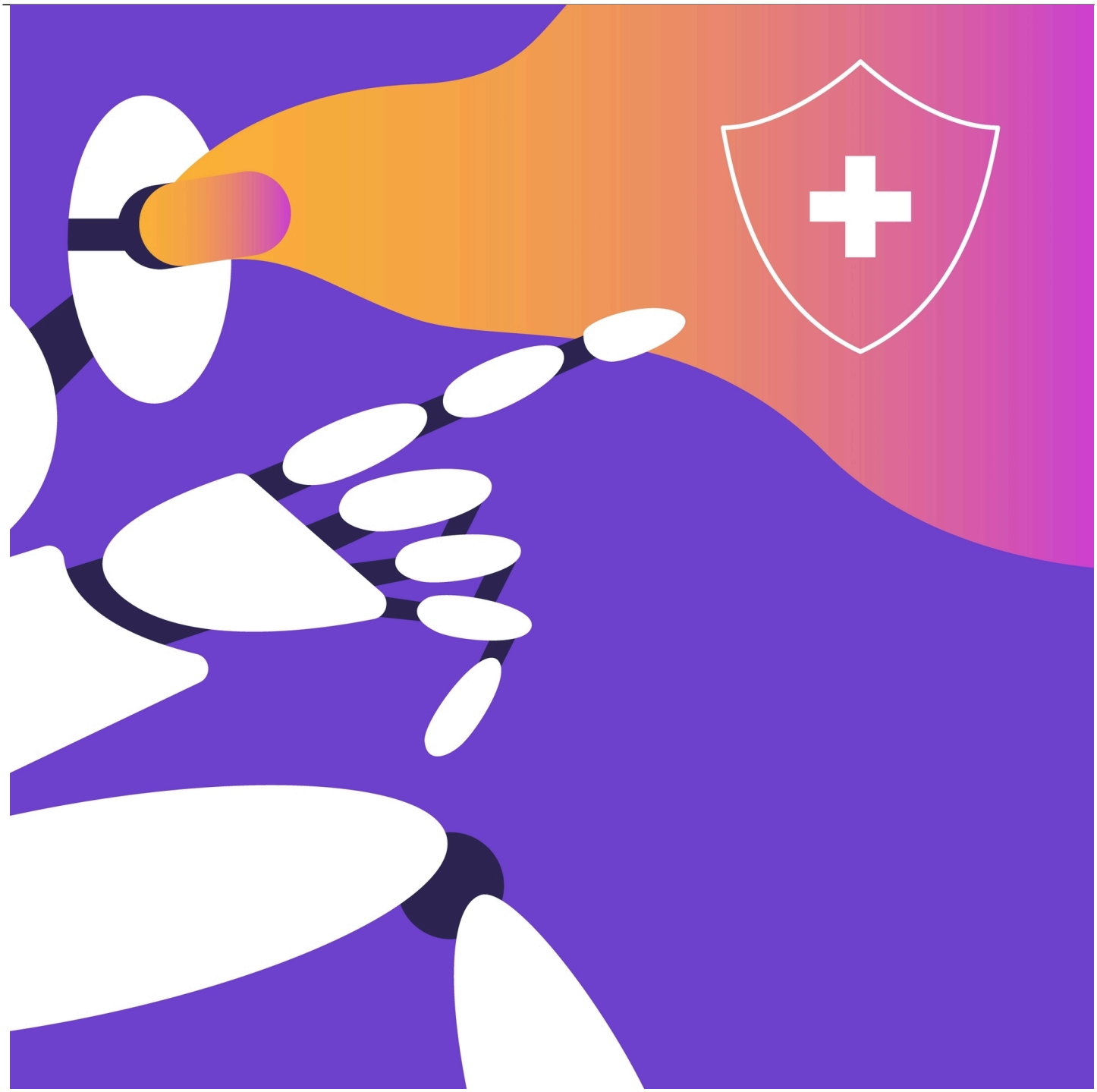
Compliance and Ethics

Information Governance

Intellectual Property

Skills and Professional Development

Technology, Privacy, and eCommerce



Banner artwork by Cranium_Soul / *Shutterstock.com*

The policy rush

AI mania has given lawyers — and especially in-house counsel — a host of new tasks and challenges.

Since OpenAI released their ChatGPT chatbot in late 2022, artificial intelligence (AI) has been an inescapable topic in business. According to, over a third of S&P 500 companies mentioned AI in their fourth-quarter 2023 earnings calls.

The buzz gets louder when the calls end. Behind every company CEO speaking to the Street about AI, there's likely a working group, task force, or even entire department discussing what the tech means for their organization. Many applications of what's commonly called "AI" raise novel, complex and ever-evolving legal issues, and lawyers are rightly in the room when evaluating these uses.

But company lawyers are also being pushed — or are pushing — to solidify guidance on these developing issues into formal "AI policies." Before inking their quills, in-house counsel should consider whether immediately fixing a policy does more harm than good.

What we talk about when we talk about AI

Puzzling about the "AI" hubbub is how little clarity there is around the word's meaning. Developers and technologists have long used the term to describe computer systems that perform a variety of human-like tasks, from making decisions to recognizing faces. Many of these systems are already integrated into our daily lives: iPhone's predictive text features, Amazon's voice assistant Alexa, and Gmail's spam filter.

Yet it's the latest wave of *generative AI* tools — tools, like ChatGPT or DALL·E 2, that produce original images, text, and other data — that has shot the term "AI" to the top of today's corporate lexicon. And during the term's speedy rise to buzzword status, "AI" now both denotes a broad technology category but also serves as shorthand for specifically GenAI tools.

The term's fuzzy meaning benefits businesses eager to ride the AI wave, as many can advertise their AI capabilities based on tech that they've used for years. For these businesses' lawyers though, the term's breadth and unsettled meaning presents challenges.

Jasper AI / *giphy*

The problem with policies

Having an organizational policy on a topic can be a great comfort, especially for in-house counsel. Well-drafted policies set clear written rules for employees to follow, which can increase efficiency, reduce risks, and promote a culture of compliance. Among their efficiency benefits, policies spare a company's legal team unnecessary work. Rather than answer the same legal questions over and over again, lawyers can point their colleagues to documents that set out the company's rules and provide answers.

With AI, however, the answers aren't always clear. One threshold issue is the definitional ambiguity discussed above: a company drafting an AI policy first needs to decide what "AI" the policy covers. If the company wants to sweep in everything currently touted as AI, then the policy will extend to traditional AI technologies that the company might have used for years, including data analytics and automation tools. That of course isn't inherently problematic. But if as a rule the company restricts or controls software labeled "AI" more than other software, the company may be regulating internal tools inconsistently. A relatively low-risk tool classified as AI may undergo significant vetting, while higher risk non-AI software may avoid the same scrutiny.

Still, the ambiguous meaning of AI isn't an insurmountable obstacle for policy-drafting. To avoid an overbroad policy, an organization might dictate different treatment for different types of AI. For instance, the org might set special rules to address issues unique to generative AI tools, prohibiting employees from inputting confidential data into the tools or from using tool outputs externally.

A more fundamental issue with AI policies persists, however. AI policies seek to fix rules for a still-developing technology governed by a growing web of laws and regulations and facing rapidly changing commercial norms. As a result, they may quickly become obsolete and fall out of step with a company's actual AI practices.

Take governmental guidance on AI, for instance. While some AI laws exist — and more will soon come — comprehensive AI legislation hasn't yet emerged. Courts likewise haven't issued clear guidance on legal issues involving AI.

The technology is developing, too. In the year and a half since OpenAI launched ChatGPT in November 2022, the chatbot has dramatically expanded its capabilities, now accepting voices and images as inputs and allowing users to create custom versions of the software. With these new updates, new issues arise.

Just as importantly, business practices around AI usage and risk are in flux. Only a year ago the most popular generative AI tools were provided to users as is, with few if any contractual warranties. But with many AI companies now offering enterprise versions and committing to indemnify users from IP claims, risk-averse organizations may become more comfortable using these tools. Even so, with many AI companies facing lawsuits, risks remain. And contracting norms are only emerging on how businesses allocate those risks among each other.

This unsettled landscape is an unsettling place for a fixed policy. With laws, technology, and commercial norms changing every day, rigid policies can become outdated shortly after they're written. If an organization's AI policy requires management to approve each new use of AI software, for instance, that process may prove cumbersome as AI usage becomes more prevalent in the company's industry and in culture. Many popular AI tools require just a few clicks for employees to access and use — but demand significant employer resources to monitor and control.

> This unsettled landscape is an unsettling place for a fixed policy. With laws, technology, and commercial norms changing every day, rigid policies can become outdated shortly after they're written.

And if actual practice changes more quickly than policy, the company risks falling out of compliance with its own rules — a situation potentially worse than having no policy at all.

You may already have AI policies

Your organization may already have policies in place that protect and safeguard personal data. Seeker1983 / *Shutterstock.com*

Perhaps the biggest reason to pause before announcing an AI policy is that you probably already have one. Even if not under that name. Many issues raised by the new tech aren't actually that new. For instance, generative AI tools can ingest a variety of data and speedily spit back answers, summaries, and analyses. This creates a risk of data incidents. If users upload confidential or sensitive information into a tool without appropriate authorization, data can be compromised or exposed — a lesson that many organizations learned the hard way.

But that danger is common to many software-as-a-service (SaaS) platforms. And organizational policies on confidentiality and data security likely already require safeguards and internal approvals before transferring confidential information outside the company. When it comes to transfers of personal information, privacy policies may set still more stringent rules. IT acceptable use policies may also restrict how employees interact with software.

Other policies may apply, too. For instance, well-drafted organizational policies on bias/representation and intellectual property should be broad and resilient enough to speak to well-documented concerns with the GenAI tools' biased and allegedly infringing outputs.

Consider a simpler path for now

For companies developing their own AI tools or large language models (LLMs), AI-specific policies remain a prudent way to address the growing scrutiny on their businesses. Lawmakers, regulators, and the broader public have all expressed concerns about the most powerful AI models, including model transparency, explainability, bias, and the use of copyrighted and personal information material for training. But for the reasons above, standalone policies on everything labeled “AI” are less appropriate for businesses merely employing AI technology.

A more efficient approach for in-house counsel is to ensure that existing policies are drafted broadly enough to cover AI-specific issues — and to the extent that they aren’t, to simply amend them as needed. Lawyers should also reinforce their confidentiality, data security, and other policies to employees through training and guidance tailored to AI concerns — even if that guidance isn’t fixed in a formal policy.

> A more efficient approach for in-house counsel is to ensure that existing policies are drafted broadly enough to cover AI-specific issues — and to the extent that they aren't, to simply amend them as needed.

Don’t get too comfortable

For many organizations, it’s premature to fix a mass of new rules for a tech category as ambiguous and evolving as “AI.” But that will likely change.

As lawmakers and regulators in the United States, the European Union, and elsewhere seek to regulate the technology, they’ll be assigning a meaning to “artificial intelligence.” The EU AI Act, for instance, set to take effect in 2026, mandates various requirements on the broad category of “AI systems,” though the restrictions applicable to a given AI system vary based on risk. Organizations subject to the Act will need to live with that definition, at least for compliance purposes.

But until definitions and practice are codified in law or widely accepted by industry, organizations should be wary of imposing rigid and comprehensive AI rules on themselves. At least for now, those rules can create more risks than they solve.

Christopher Wlach

Senior Director, Legal

Acxiom

Chris Wlach is the senior director, legal of Acxiom. Before moving in-house he focused on complex commercial litigation at Arnold & Porter. He is a certified information privacy professional (CIPP/US) through the International Association of Privacy Professionals. He also chairs the board of HEART, a humane education nonprofit.