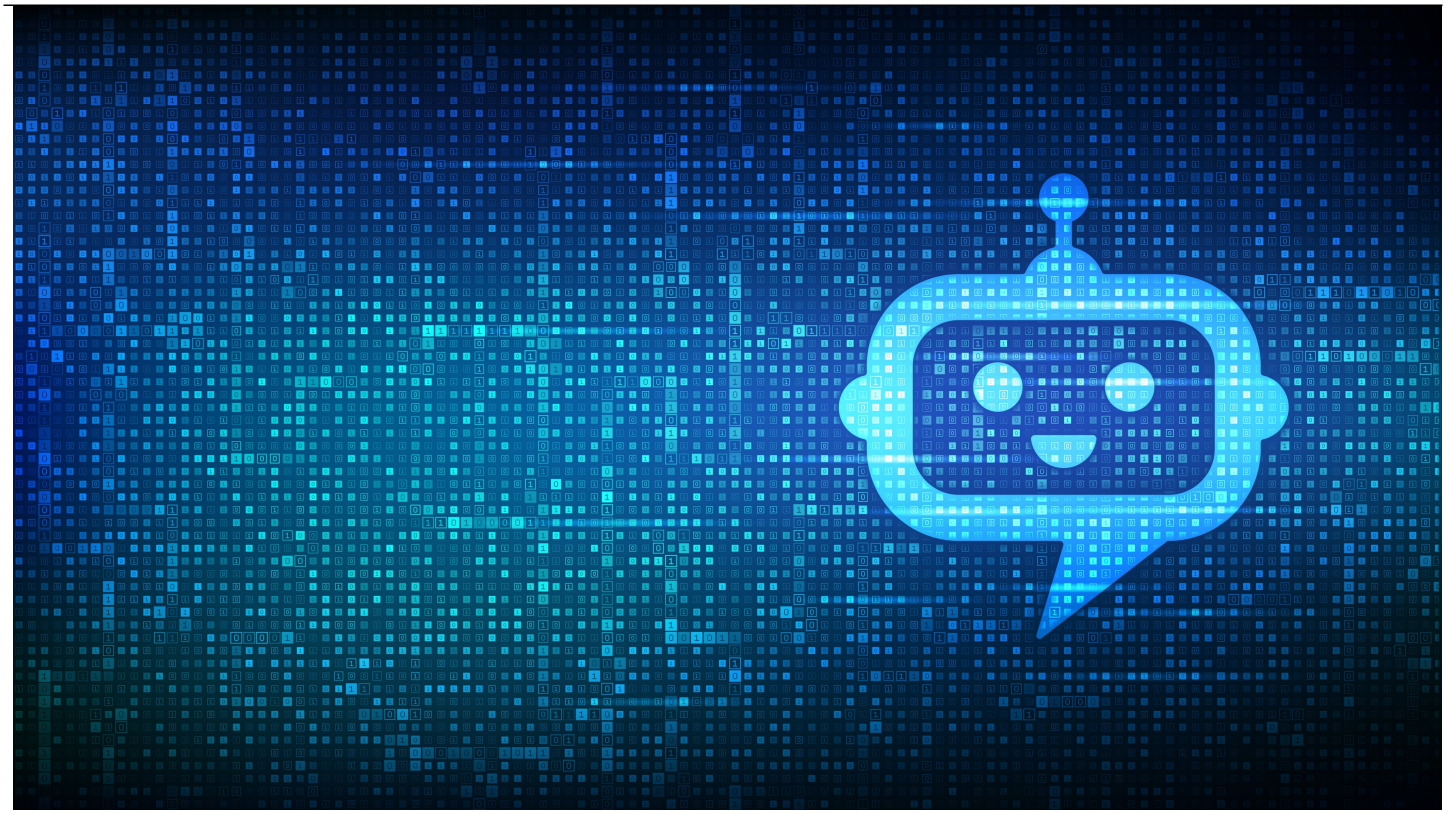
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Employees Are Using Chatbots — Make Sure Your AI Use Policy Works

Technology, Privacy, and eCommerce



Banner artwork by Iurii Motov / *Shutterstock.com*

Artificial intelligence generative software such as ChatGPT, Bard, DALL-E, Stable Diffusion, and Midjourney (AI chatbots) is everywhere these days, and as in-house counsel, you need to start addressing the organizational risks that arise when your staff starts to use these services against the business objectives to stay competitive.

Risks might include:

- Performance risks, e.g., errors and biases;
- Security risks, e.g., false, deceptive, misleading, “deepfakes” data and information, and the potential of cyber intrusions into your organization’s IT systems and network;
- Business risks, e.g., reputational and misalignment with your organization’s values;
- Control risks: loss of control of valuable data, inability to detect unintended outcomes, loss of privacy; and
- Intellectual property, such as trade secret and copyright risks.

Below, we outline steps you should consider when you start developing your organization’s policy on generative AI tools, including chatbot usage.

1. You need to get started.

Chances are your staff is already using AI chatbots, seeking to experiment with this new and exciting technology, but having little or no appreciation for the various risks associated with such use. As in-

house counsel, it is imperative to provide your firm with guidance, in order to manage the competing dynamics of risk versus efficiency and productivity. In this instance, addressing the opportunity proactively is more advantageous than inaction.

Use proper guidance with your team to safely manage and mitigate any potential risks associated with AI chatbots.
hProStockStudio / *Shutterstock.com*

> As in-house counsel, it is imperative to provide your firm with guidance, in order to manage the competing dynamics of risk versus efficiency and productivity.

Check out ACC's Sample Artificial Intelligence Usage Policy

2. Educate top management.

At this point, there have been enough articles published in popular media imploring top level management to be aware that AI chatbots are everywhere. The reality that people are probably already using the technology in your organization, or the risks that are particular to your operations, may not be top of mind. You need to educate them on the specific risks your organization faces if guidance is not given. Prepare talking points that address each of the following areas (almost all of which are probably applicable):

- Privacy
- Data and trade secrets security
- Copyright and trademark issues
- Bias contained in AI (e.g., HR products and activities)
- Coding risks
- Breach of contractual obligations regarding data use and protection
- Violation of regulatory obligations (e.g., HIPAA)
- Errors/output integrity
- Cybersecurity enhanced risk

This education process should extend to your board or your board risk management committee to assist in their oversight roles and address changing disclosure regulations over cybersecurity practices.

3. Acknowledge why people want to use AI. Commit to examining risks and rewards.

It is very easy for lawyers to talk about risk without acknowledging that there are some real potential productivity gains. Rather than starting with a position of “no usage ever” (although an immediate pause on usage could be reasonable), commit to examining the use instances and working with internal departments to determine what the proper balance of risks and rewards are for your organization. Try to figure out if there are ways to mitigate risks. A number of AI products are starting to roll out enterprise solutions with greater security features.

4. Assemble a team to examine the organizational risks and needs.

This is not the time for legal to develop policy in a vacuum, and you will need to work closely with various internal constituencies depending on your company’s profile, including your IT team, developers and product teams, HR, finance, investor relations, business generators, risk management, and others.

You should engage people at all levels (and ages) of the organization to find out what is actually happening (or desired) before you can develop a policy that can be actually implemented. The enterprise-wide effort will be more successful if you seek to engage a broader base of internal stakeholders who may be thinking about how to use this technology to advance their business objectives.

It is in the best interest of in-house counsel to engage with the entire organization to decipher risks and needs before moving forward with developing an AI policy.
GoodStudio / *Shutterstock.com*

[Check out ACC's New AI Resource Library]

> You should engage people at all levels (and ages) of the organization to find out what is actually happening (or desired) before you can develop a policy that can be actually implemented.

5. Review regulatory and contractual obligations particular to your organization.

Although everyone may want access to new technology, there may be regulatory barriers or prohibitions. For instance, you may not be able to use an AI chatbot and be compliant with HIPAA health privacy regulations. You might be subject to employment law violations if you make certain HR decisions based on biased AI technology; e.g., recently enacted regulations in New York City. GDPR might prohibit you from allowing PII (personally identifiable information) to be used for training AI chatbots. Make sure you consider the regulatory frameworks that might impact your company's usage.

6. Determine who will "own" the policy.

To implement a policy, you will need support from top level leadership of the organization, with an understanding of who will own and be responsible for the policy. Will legal, IT, security, compliance, or some other group created during the policy drafting phase be responsible? Like any new company wide process, consider test driving it across various departments and at various levels in the organization. Seek feedback and embed suggested improvements.

The situation will be dynamic and your AI team should monitor ongoing developments and impact in order to address possible policy changes. For example, if you are allowing usage in certain instances, how do you obtain permission? Who will they contact if they want a use instance not explicitly addressed in the policy?

In the event of a possible policy change, an AI team should always be up to speed and aware of any ongoing developments. VectorMine / *Shutterstock.com*

> Like any new company wide process, consider test driving it across various departments and at various levels in the organization. Seek feedback and embed suggested improvements.

7. Create a policy for your vendors (new and renewals).

It is not just your staff who can create risk for your organization by using generative AI tools. Your vendors are likely using the technology as well, possibly creating risk for your organization. For example, a number of organizations are updating their terms of service, seeking consent to “train” their technology when you use their products. What does “train” mean? What will the vendor do or use?

You should also consider contractual obligations in vendor contracts to explicitly prohibit use of any company data or information to be used for the vendor’s training or other business objectives. Asking questions about how a vendor will use your company’s data and information should be part of the

normal vendor due diligence process, and AI use will be no exception.

8. Acknowledge that your policy is going to be interim.

Once you get your policy in place, do not imagine your work will be done. AI technology is evolving too quickly for anything to be permanent. Resolve to keep learning, evaluating and be ready to change.

Join ACC

Robert Falk

General Counsel

Truth Initiative

Rob Falk is general counsel and corporate secretary of Truth Initiative. He has previously served on ACC's global board of directors and as chapter president of ACC National Capital Region.

Margo Lynn Hablutzel

Senior Counsel

Gainwell Technologies LLC

Margo Lynn Hablutzel is senior counsel for Gainwell Technologies LLC, a healthcare technology and services company headquartered in Irving, Texas. Hablutzel has a bachelors degree from the University of Chicago; a juris doctorate from

IIT Chicago-Kent College of Law; a MA in Intellectual Property Law from John Marshall Law School (now the University of Illinois at Chicago Law School); and is a certified information systems security professional through ISC2. She is or has been active in other bar associations including the Chicago Bar Association, the Dallas Bar Association, the Illinois State Bar Association, the American Bar Association, and the International Trademarks Association. Hablutzel is a frequent writer and speaker on topics including intellectual property and cybersecurity for both bar associations and layperson organizations, and has found herself a fluent translator between legal, technical, and layperson communities.

Heather Peck

Technology/IT Counsel

Inspire Brands, Inc.

Heather Peck is vice president, technology/IT counsel at Inspire Brands, Inc. and leads the legal team that supports IT and technology initiatives at the restaurant company. She earned a JD/MA in East Asian Studies at Washington University in St. Louis.

Jonathan Yellin

General Counsel

Charles River Associates

Jonathan D. Yellin has been the general counsel of CRA International, Inc., d/b/a Charles River Associates, a leading global consulting firm specializing in economic, financial and management consulting services, since joining CRA in 2004. Immediately prior to joining CRA, he was a senior partner in the Insolvency and Restructuring practice at Riemer & Braunstein LLP, based in Boston, MA. Yellin received his juris doctorate *cum laude* from the University of Miami School of Law in 1988 and his bachelor of arts degree from The George Washington University, School of Public and International Affairs, in 1985. He is currently the chair of the subcommittee on artificial intelligence for the ACC's IT, Privacy & eCommerce Network.