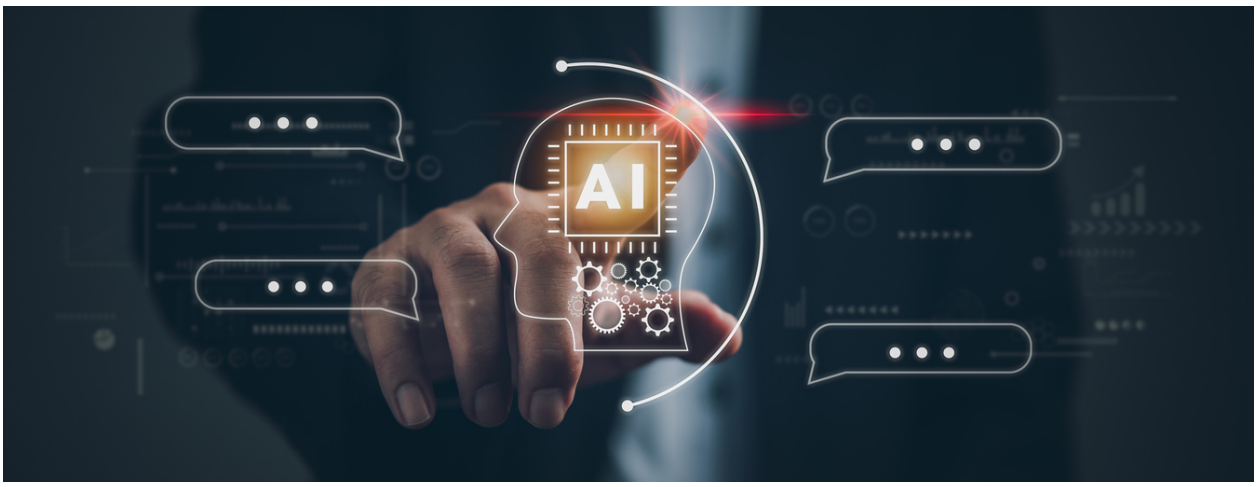


When it Comes to Generative AI, Ignorance is not Bliss: Three Risks Your Business Faces by Failing to Regulate Workplace Use of Generative AI.

Richard L. Hathaway

OpenAI, the private AI research and deployment company, released ChatGPT to the public in November 2022. ChatGPT is a generative AI chatbot that enables human-like conversations. Its availability and ease of use have made it extremely popular—garnering a record-breaking 100 million users by the end of January 2023. ChatGPT's popularity has also spurred other tech companies to launch generative AI applications. The speed with which generative AI has spread is remarkable and, for some employers, alarming.

Companies across various industries are reacting to generative AI's infiltration into their offices. Numerous banks, defense contractors, and telecommunication companies have banned ChatGPT in their offices. Gartner recently surveyed human resources professionals concerning ChatGPT's spread into the workplace. Nearly half of those polled said they were formulating employee guidance on using ChatGPT. In contrast, about one-third said they did not intend to issue workplace ChatGPT usage policies.[1]

[1] Mukul Sharma, "ChatGPT ban? Companies formulate new policies to regulate use of Artificial Intelligence," https://www.wionews.com/technology/chatgpt-ban-companies-formulate-new-policies-to-regulate-use-of-artificial-intelligence-574401, Updated, March 22, 2023, (Last visited, April 11, 2023).

There are Two Important Realities about generative AI in the workplace: (1) Your employees already use ChatGPT or other generative AI at work, and (2) There is Little or No Regulatory or Legal Framework to Protect Businesses.

Widespread availability and ease of use have tempted employees across every industry to find ways to use generative AI at work. Recent surveys conducted by Fishbowl and Monster.com reveal that as much as fifty percent (50%) of workers polled have used generative AI to perform or automate tasks at work. However, the vast majority of those workers, almost seventy percent (70%), have yet to tell their employers.[2] Cyberhaven Labs, a cybersecurity company that offers tools that identify and protect against cyber threats to their client's data, reports that usage of generative AI applications by employees at companies, specifically ChatGPT, continues to grow exponentially.[3] With or without policies in place, short of an outright ban on its use at work, it is inevitable that some of your employees will use, or are already using, generative AI to assist with their work.

The broad reach of generative AI's capabilities to create and continuously learn challenges the application of existing regulatory and legal frameworks. Potential uses of the technology implicate many current laws and regulations governing products, privacy, intellectual property, and countless industry-specific regulations. Because these existing laws and regulations could not anticipate generative AI, they leave a lot of open questions and very few answers. Some governing bodies have recognized the regulatory and legal vacuum and have started proposals and initiatives. This year China and the European Commission separately proposed draft measures or regulatory frameworks aimed at AI developers, distributors, and users. On April 11, 2023, the National Telecommunications and Information Administration (NTIA), a U.S. Department of Commerce branch, formally requested input on what policies should shape the AI accountability ecosystem. And while some states have passed legislation concerning specific uses of AI technology, most are consumer protection-based. None are considered a framework aimed at regulating generative AI in the workplace

[2] Lindsay Ellis, "ChatGPT can save you hours at work. Why are some companies banning it?," https://www.wsj.com/articles/despite-office-bans-some-workers-still-want-to-use-chatgpt-778da50e, last updated, March 22, 2023, (Last visited, April 13, 2023).

[3] Cameron Coles, Cyberhaven, "11% of data employees paste into ChatGPT is confidential,"https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt/ last updated, April 19, 2023, (Last visited, April 21, 2023).

Turning a blind eye to generative AI could be costly.

Whether your business intends to take advantage of this technology's benefits, it must pay attention to the risks associated with the absence of policies and training to address generative AI usage at the workplace. Companies that are not proactive in analyzing this technology and deploying procedures regulating its use are likely to face three significant risks:

(1) Unauthorized disclosure of intellectual property, confidential information, and trade secrets;
(2) Liability for violation of privacy, consumer protection, or other laws; and
(3) Lack of reliable monitoring, auditing, or internal checks.

Fueled by the certainty that employees are using or will use generative AI at work and the current lack of regulatory and legal frameworks aimed explicitly at generative AI applications, these risks are genuine and could prove extremely costly.

Risk Number 1: Unauthorized disclosure:

The biggest risk businesses face from generative AI is the unauthorized disclosure of confidential information, trade secrets, or other intellectual property. Employees can easily share information with ChatGPT (or any other generative AI) by cutting and pasting parts of documents into the prompt. Such disclosure could result in the loss of trade secret status or additional protection and create contractual and other types of liability. Data security service Cyberhaven recently reported that just over three percent (3.1%) of workers they monitor had disclosed confidential information to ChatGPT. It also noted that the risk unmonitored and unregulated employees pose for unauthorized disclosure is significant and growing. "The average company leaks confidential material to ChatGPT hundreds of times weekly. ChatGPT is incorporating that material into its publicly available knowledge base and sharing it." [4]

[4] Cameron Coles, "The problem with putting company data into ChatGPT," https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt/ Updated March 21, 2023, (Last visited, April 13, 2023) (emphasis added).

Risk Number 2: Violations of privacy, consumer protection, and other laws:

Current data privacy and protection laws regulate and protect the privacy of consumer personal, financial, and protected health information. Businesses that handle this information as a necessary part of their day-to-day business should already be familiar with and have policies and training addressing compliance with laws such as the General Data Protection Regulation (GDPR) in the European Union, the federal Health Insurance Portability and Accountability Act of 1996 (HIPPA), and various state privacy acts such as the California Consumer Privacy Act (CCPA). With one simple act of cutting and pasting protected data into generative AI, an employee may breach these protection laws and create liability for your business. Considering the high frequency with which the average company leaks confidential information to ChatGPT, your business could rack up many breaches before it finally discovers employee misuse.

Depending on the "Terms of Use" for the generative AI tool and the data used to train it, unregulated employee use of generative AI can result in liability for your business. As workers rely more on generative AI, they are less inclined to verify the accuracy of the technology's answers. Most AI applications disclaim representations and warranties for the accuracy of their tools' answers. They may also fail to recognize when generative AI provides results that infringe on existing copyrights, trademarks, or patents. Employees' mistakes relying on generative AI alone add a layer of legal risk to your business.

Risk Number 3: Lack of Reliable Monitoring, Auditing, and Internal Checks:

Unmonitored employee use of generative AI can effectively "undo" your procedural and digital safety mechanisms. Employees accessing these tools via the internet or a proxy can allow them to interact with all sorts of information, making it difficult to monitor the information accessed. Detecting and preventing unauthorized access to confidential information or other improper use of generative AI is also problematic when there is no training or policy concerning its use at work. Even in the best circumstances, the need for more transparency concerning some generative AI algorithms or machine learning models makes it difficult for businesses to audit their decision-making process. The unregulated use of generative AI makes the audit process more complicated and, depending on the extent of its use, more costly.

A proactive approach is critical to minimizing these risks.

Businesses should take a proactive approach to minimize the risks associated with unregulated generative AI use while maximizing its productivity benefits. Depending on the potential risks and liability exposure, it may serve some businesses by implementing a temporary ban on generative AI use while assessing the situation and developing a plan. With or without a temporary ban, businesses should determine the extent to which generative AI is currently used and decide how they want to use it.

Having decided how the business wishes to utilize generative AI, if at all, businesses should then:

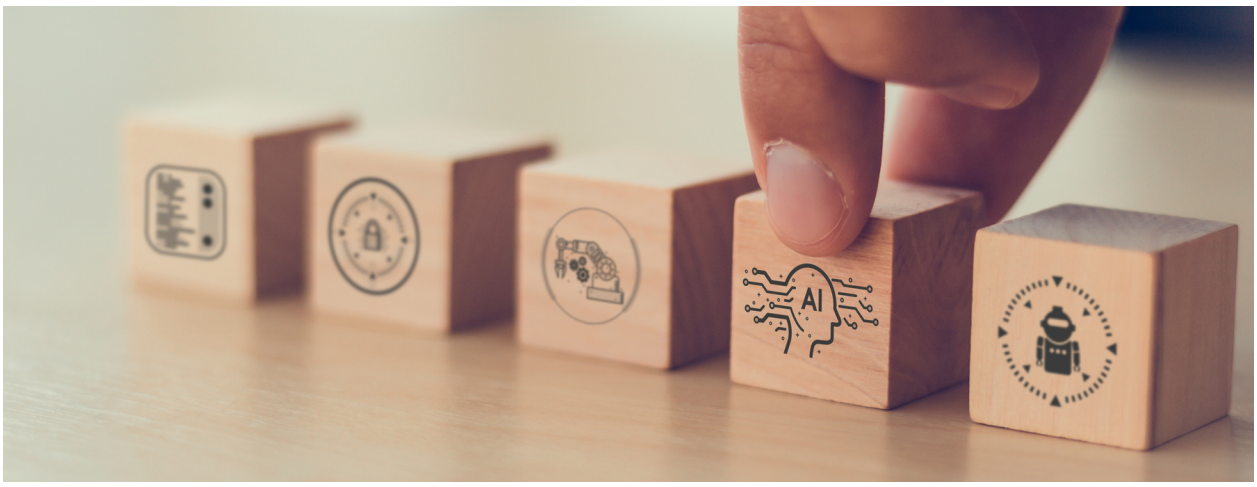
- Institutionalize the use of generative AI by carefully choosing applications that have terms of service, privacy policies, and security measures that complement the business' specific needs and requirements;

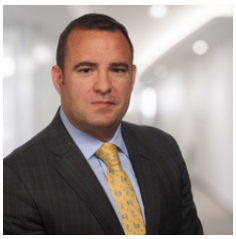
- Update compliance policies and training to educate employees about the types of information that employees can share with generative AI and identify the types of generative AI applications they are permitted to use;

- Require access controls, user authentication, and other measures to ensure the selected generative AI application can only access the information needed to perform their roles;

- Collaborate with the generative AI provider to reliably monitor and audit the use of generative AI to ensure compliance with the company's policies, guidelines, and current legal requirements.

Because generative AI is a rapidly evolving technology, having a dedicated person or group of people responsible for executing and updating your generative AI plan is also essential. By taking these measures and remaining flexible and proactive, your business is on its way to minimizing the risks unregulated generative AI use brings to the workplace.





About the Author

For more than twenty years, **Richard L. Hathaway** has litigated non-competition, non-solicitation, trade secrets, and other matters protecting business innovation. He has successfully enforced his business clients' agreements and rights in Texas state or federal court and arbitration. He has recently obtained a multi-million dollar arbitration award for a business against a former employee for misappropriating trade secrets. He and his team can assist your company in protecting its trade secrets via a policy and training review or aggressively pursuing available legal avenues. He is available via email at: Rhathaway@krcl.com and phone at: 214-777-4270.