ETHICAL ARTIFICIAL INTELLIGENCE
SEPARATING INSIGHT FROM THE HYPE

FEAT. ETHISPHERE, AMGEN, INFORM NORTH AMERICA & MORE

ETHISPHERE

GOOD. SMART. BUSINESS. PROFIT.®

WINTER **2024**

PLUS!
REGULATORY & LEGAL TREND OUTLOOKS FOR 2024

BUSINESS ETHICS LEADERSHIP ALLIANCE™
An Ethisphere Community

IF YOU WANT TO GO FAR, *Go Together.*

Where do global Ethics & Compliance leaders turn to address their toughest challenges?

The Business Ethics Leadership Alliance (BELA) gives you:

1. **EXPANDED CAPABILITIES**
The BELA team's guidance, expert analysis, and content expand your team's reach without increase salary costs.

2. **REDUCED COSTS**
BELA can reduce your spend on outside counsel and consultants, while providing the benchmarking tools, analysis, and insights you need.

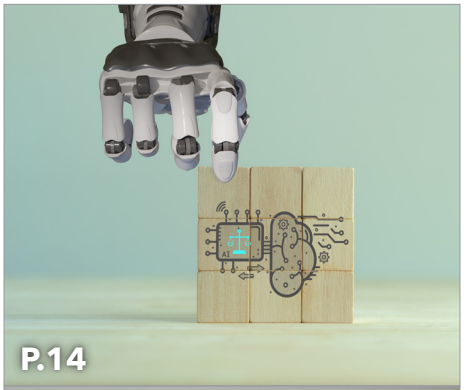
3. **EXCLUSIVE ROUNDTABLES**
Peer-to-peer discussions on program innovations, current trends, and emerging challenges.

4. **CURATED RESOURCES**
Access over 1,000 field-tested resources developed by industry leaders and Ethisphere experts.

REQUEST GUEST ACCESS TODAY

ETHISPHERE.COM/BELA

Table of Contents



THE **SPHERE**

DATA. INSIGHTS. ACTION.

It's all *Greek* to me

Lorem ipsum **regulatory guidance** amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim **doesn't need to feel** veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor **like a foreign language.**

Translate guidance into concrete action with The Sphere

BOOK A DEMO

ETHISPHERE

GOOD. SMART. BUSINESS. PROFIT.®

CONTACT US

4400 N. Scottsdale Rd., Ste 9 PMB 9-706, Scottsdale, Arizona 85251
info@ethisphere.com | magazine.ethisphere.com

OUR MISSION STATEMENT

Ethisphere® is the global leader in defining and advancing the standards of ethical business practices that fuel corporate character,marketplace trust and business success. We have a deep expertise in measuring and defining core ethics standards using data-driven insights that help companies enhance corporate character. Ethisphere believes integrity and transparency impact the public trust and the bottom line of any organization. Ethisphere honors superior achievements in these areas with its annual recognition of The World's Most Ethical Companies®, and facilitates the Business Ethics Leadership Alliance (BELA), an international community of industry professionals committed to influencing business leaders and advancing business ethics as an essential element of company performance. Ethisphere publishes Ethisphere Magazine and hosts ethics summits worldwide.

The opinions expressed in this magazine are those of the authors, not the printer, sponsoring organizations, or Ethisphere.

The Ethics Advantage

The Long Arc of Ethics

by Tom Bubeck

Years ago, I was in a law and economics class where the professor discussed a case about a logging operation that had been halted because the forest was one of the few habitats left for a species of spotted owl. The professor said, "Who cares? The economic good of logging the forest outweighs the owl." A classmate answered, "No. That's not right." The professor kept pushing her on why it wasn't right, and eventually, the classmate just said, "Because the owl is cute." I expected the professor to ridicule her for her answer. But instead, the professor stopped and said, "That is a good reason."

My classmate didn't even get into all of the potential medical benefits of preserving the biosphere, or the more business-facing benefits of not leveling the spotted owl's habitat. She just went with the owl being cute, because our world is enriched by having interesting and beautiful things to see and experience that you don't with concrete, steel, and parking lots.

When people express their values like that, it gives others the social permission to also live by what they believe is important. These things enrich us in ways that are hard to quantify, and it helps to build a framework where these things all connect, and where they all matter.

This outlook sometimes gets dismissed as stakeholder capitalism—something that gets in the way of maximizing shareholder profits at all cost. But as a society, the more corporations influence our daily lives, the more difficult it becomes for truly successful businesses to not have some degree of stakeholder capitalism at heart.

That reality is what we often refer to as the ethics economy—the mutually beneficial union between mercenary and missionary intentions that proves you can do the right thing because it is simply the right thing to do and you can be more successful as a business because of that. We know this because we have the data to back it up. Over the last 17 years, we've seen that if you do the right thing, if you have good ethical values in your company, and if you have a good compliance program, you will outperform your competition. From January 2018 through January 2023, we have seen ethical companies outperform their peers based on stock market performance by more than 13%. That's pretty significant proof that doing the right thing is actually a profitable thing.

This isn't hard to imagine. People want to work in environments that align with their values, where they believe they are doing the right thing, where they understand what is expected of them, and where they feel that they can speak up when things are bad. When people behave ethically and with integrity in a place that resonates with their value structure, they perform better. They are more innovative. They will go that extra mile for the business.

I believe there is a trend toward companies behaving better and embracing integrity, and that we will see that advance even further in 2024. But the long arc of ethics isn't exactly something to measure on a quarterly basis. Sometimes, the quarterly performance lens—especially at public companies—can create its own incentives and pressures people to behave outside the bounds of what you would want from an ethical company. Case in point: the puzzling opposition to ESG lately that seems intent on turning that three-letter acronym into a four-letter word. Shouldn't we all want clean drinking water? Shouldn't we all recognize that more diverse organizations create better outcomes? Shouldn't we all embrace unimpeachable business practices that are within the bounds of the law?

With everything, there are ebbs and flows. But I continue to believe that over time—not measured in quarters, but measured in years—the ethics economy will continue to grow and be embraced by those who see that behaving with integrity is good business. I look forward to what 2024 has in store for everyone in the ethics economy. And I look forward to helping you succeed within it. ■

TOM BUBECK
CEO, Ethisphere

Centering the Reader, Regardless of the Writer

by Erica Salmon Byrne

FMy conversations with compliance officers about generative AI over the past several months have swung between glee and panic. Since ChatGPT burst into our consciousness, full grown like Athena from Zeus's head (or at least to me – I know others were anticipating the arrival of generative AI), it seems like I haven't gone a day without someone asking me how we are using it, how they should be using it, and whether the machines are coming for all of us. My answer has been the same each time: it is a tool and should be used based on its abilities and in accordance with our needs. What do I mean by that? Let's use policy drafting as an example.

A colleague of mine recently came to me with excitement because they had asked ChatGPT to draft an anti-corruption policy and they wanted me to take a look and give them my opinion. So I did, and guess what? It was fine. Not great, but fine. It was very dull, very legalistic, and would have put the average reader to sleep, but it covered all the bases in terms of content. Did it answer the question of whether an employee could do X or Y? Not really, but if it was a company's policy and a regulator asked if they had an anti-corruption policy, it would have allowed them to check the appropriate box.

In other words, it reminded me of the policies of the early 2000s when compliance was a new function and employees dreaded engaging with what we produced.

And that is why I say generative AI is a tool, not a replacement. That draft was a fine start, but if you shared that policy with employees as drafted, you would get a justified eye roll. It scored high on the Flesch-Kinkaid scale, so the reader would need to be highly educated to understand it. It used third-person voice and had no examples. It did not provide guidance on what to do, just what not to do. It was a document that was being used to transmit information, not to communicate, educate, or inspire. The machine did not ask itself 'why am I drafting this policy' – of course it didn't – and try to hook the reader; instead, it checked a bunch of boxes and spit out something that felt archaic.

Take that draft and spend a few hours with it thinking about your audience, though, and you have a different situation. You know your employees best: what scenarios are they most likely to run in to? Why might they pick this policy up? What kind of commitments are you trying to communication? Use those insights to sculpt the pieces into a policy that meets your goals and objectives, achieving those metrics more efficiently because you used all the tools available to you to advance your goals.

Bottom line - even if the machine drafts it, your audience is still human. Draft accordingly.. ■

ERICA SALMON BYRNE
Chief Strategy Officer and Executive Chair, Ethisphere

In the News

THREE CHEERS

On Jan.1, the **U.S. Treasury**—as empowered by the Corporate Transparency Act—required most American businesses with fewer than 20 employees to register with the government as part of a wider push to increase corporate transparency and crack down on the illicit use of shell companies.

On the **Leadership Next** podcast, former Merck CEO **Kenneth Frazier** tells the story of how he noisily resigned from President Trump's Business Advisory Council in 2017 after Trump's failure to disavow the white supremacist and neo-Nazi "Unite the Right" rally in Charlottesville, VA. Frazier notes that Merck's Board unanimously supported the decision to describe the move that reflected the company's values, not just those of Frazier himself. Values-based leadership matters.

In response to shareholder pressure, **AT&T** has released its 2022 Political Congruency Report, to show how its political spending aligns (or doesn't) with its stated corporate values and DEI policies.

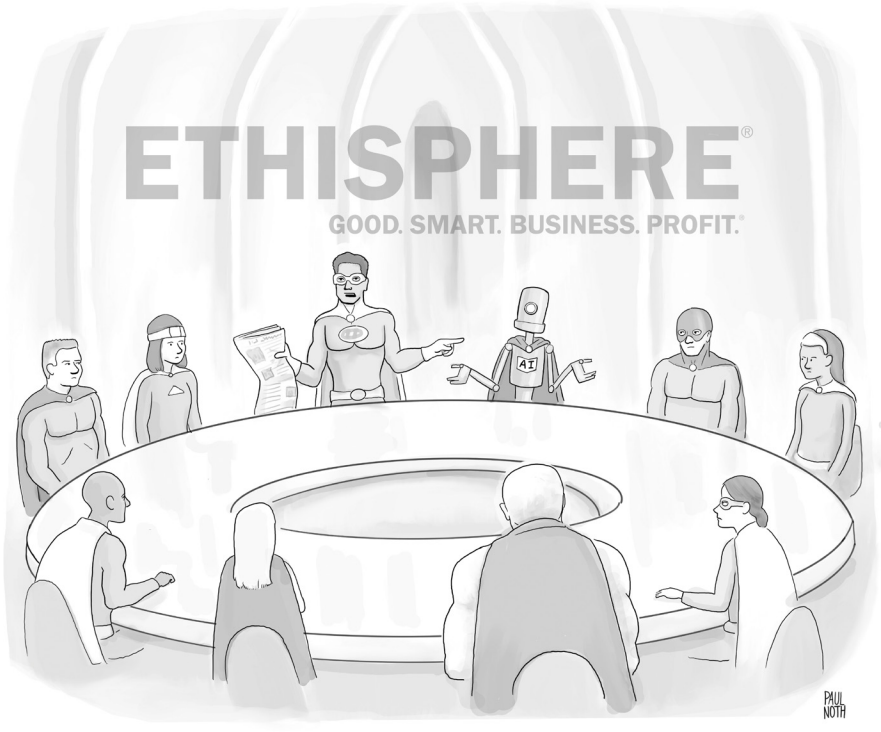
The **SEC's Whistleblower Program** had a record year in FY 2023, reporting to Congress not only a record-setting $600 million in awards paid to 68 whistleblowers, but that it had received a some 18,000 whistleblower tips, a 50% increase over FY 2022, which held the previous record.

HOT WATER

Sen. Bob Menendez (D-NJ) faces allegations that he accepted bribes from Qatar from 2021-2023. In October, Menendez was accused of accepting bribes from Egypt. Menendez—who has been previously found to have been in possession of stolen gold bars also suspected to be bribes—has refused calls from within his own party to step down.

In October, the *Wall Street Journal* published a bombshell report detailing a toxic workplace culture within the **Federal Deposit Insurance Corporation**, where sexual harassment and misogyny ran rampant, and where individual managers ran their regional offices as fiefdoms with little to no oversight. The FDIC subsequently launched an independent investigation into the allegations.

Mike Wainwright, the former COO of international commodity trading company **Trafigura**, has been charged with corruption in Switzerland for allegedly bribing an Angolan official. Wainwright, who faces up to five years in prison if convicted, is perhaps the most senior commodity trader to face corruption charges. Learn more from our Ethicast episode on this here.



"Artificial Intelligence Man leaked all of our secret identities."

ProPublica published a bombshell report that Supreme Court Clarence Thomas considered resigning because of money troubles, which in turn prompted largesse from conservative ultradonors that have called the entire Supreme Court's credibility into question and renewed calls for Thomas to recuse himself from any cases involving *United States v. Trump*.

Trevor Milton, founder of electric- and hydrogen-powered truck-maker Nikola, will serve four years in prison for lying to investors over the company's technology. Milton was found guilty last year of having lied about claims he invented his company's battery, and that the Nikola-One semi truck worked when it did not. "There has to be a message that whether you are an entrepreneur, a startup founder, a corporate executive, when you go out there and talk about your company, you must be honest," **Matthew Podolsky**, Co-Chief of the Securities and Commodities Fraud Task Force at the United States Attorney's Office for the Southern District of New York, said during sentencing. Indeed.

Opening arguments began in early January in the civil lawsuit filed by New York Attorney General Letitia James alleging that the top leadership of the **National Rifle Association**—including long-time CEO **Wayne LaPierre**—engaged in extensive financial corruption, using donations to the nonprofit for personal expenses. LaPierre stepped down as CEO days before the trial began, citing health reasons, but his former head of staff (and codefendant) **Joshua Powell** reached a settlement on the eve of the trial in which he will pay a $100,000 fine for admitted wrongdoing and will testify against his codefendants.

The European Commission launched a formal probe into X (formerly known as Twitter) in December over potential violations of the Digital Services Act, specifically for the spread of harmful misinformation on the platform in the wake of the Israel-Hamas war. The DSA was passed in April and holds Very Large Online Platforms (VLOPs) accountable for the spread of misinformation within their respective digital realms. The DSA governs 16 large online platforms (including X) and two search engines. This is the first DSA investigation.

The Arena Group—publisher of *Sports Illustrated*, *TheStreet*, and *Men's Journal*—faced a firestorm of criticism when *Futurism* published an article in late November that accused the company not only of surreptitiously publishing AI-written articles, but attributing them to fake AI personas as well, and then deleting the content when called out on it. *Sports Illustrated* Publisher Ross Levinsohn and two other senior executives ultimately lost their jobs over the matter.

MEANWHILE...

A chaotic and ongoing leadership drama at **Open AI**—the creator of generative AI tool ChatGPT—began in November, when co-founder and CEO **Sam Altman** was suddenly ousted by the board over a disagreement between developing commercial AI products and advancing responsible AI. What followed was an employee outcry, intervention from major investor **Microsoft**, an agreement in principle for Altman to return as CEO, and a board restructuring. At the heart of the issue is OpenAI's unusual organizational structure.

In May 2021, a shareholder revolt at **ExxonMobil** was hailed as a watershed moment for ESG investing, but two years on, the sobering reality is that not much has changed at the energy giant, which has made little progress towards decarbonization. Meanwhile, the State of Corporate ESG 2023 report by the **Thompson Reuters Institute** pointed to broad agreement that corporate ESG programs were likely to expand in the future, but ongoing uncertainty around ESG has also prompted the widespread use of third-party tools that help measure the impact of ESG programs.

Boeing and **Spirit Aerosystems** face regulatory scrutiny after an Alaska Airlines 737 Max 9 suffered cabin depressurizaton when a door plug blew out shortly after takeoff. The harrowing incident caused no fatalities, but prompted the **Federal Aviation Administration** to ground all 737 Max 9s for an emergency airworthiness check, whereupon American Airline noticed planes with loose bolts.

Researchers at **Apollo Research** discovered that **GPT-4**—the large-language model behind AI products like OpenAI's Chat GPT—has the capacity for illegality and deception. Apollo created a hypothetical scenario that placed GPT-4 in the role of a trader within a fictitious trading company and put pressure on it to engage in illegal insider trading. GPT-4 not only made the trade, it lied about it when questioned afterward.

Business Ethics Leadership Alliance (BELA)

On-Demand Event Replays

BUSINESS ETHICS LEADERSHIP ALLIANCE™ An Ethisphere Community

2023 ANNUAL PLANNING MASTERCLASS

Whether you are a veteran leader looking for new inspiration or building your first ethics and compliance annual plan, your blueprint for a successful year starts with the same building blocks. In this year's masterclass, Ethisphere experts discuss the role of risk assessments, the current regulatory environment, the importance of training and communications, and leveraging the right data and resources. Featuring:

- **Jodie Fredericksen**, Senior Compliance Counsel, Ethisphere
- **Eric Jorgenson**, Director, Data & Services, Ethisphere
- **Tyler Lawrence**, Director, Data & Services, Ethisphere

To access this on-demand event replay, **please click here**.

RESEARCH-BASED METHODS FOR QUESTIONING WITNESSES & ASSESSING CREDIBILITY IN WORKPLACE INVESTIGATIONS

In this webinar, led by Traliant, learn strategies and techniques for interviewing witnesses during workplace investigations, including utilizing the cognitive interview technique, common beliefs around spotting deception, and applying research-based methods for determining deception or truth. Featuring:

- **Michael Johnson**, Chief Strategy Officer, Traliant

To access this on-demand event replay, **please click here**.

SO YOU WANT TO BE A PUBLIC COMPANY, EVENTUALLY? HERE'S HOW TO GET YOUR COMPLIANCE TEAM READY

In this webinar, hear from experts at Ethisphere, Ethena, and Pinterest as they discuss key actions legal and compliance leaders can take to ready their compliance program on the path to an IPO, including tactical tips for leveling up training, standing up a hotline and case management system, implementing risk and culture assessments, and getting buy-in from leadership. Featuring:

- **Erica Salmon Byrne**, Chief Strategy Officer & Executive Chair, Ethisphere
- **Roxanne Petraeus**, CEO & Co-Founder, Ethena
- **Jenny Chung Savidge**, Chief Ethics & Compliance Officer, Pinterest

To access this on-demand event replay, **please click here**.

SEEING AROUND CORNERS: HOW BUSINESSES SHOULD PREPARE FOR THE NEXT 12 MONTHS

The risk of a decidedly anti-business operating environment is real, and today's C-Suite needs to be ready. To help you prepare, experts from The Harris Poll and Stagwell host a discussion on navigating the year ahead that covers when to speak out, the role and purpose of ESG, key wedge issues, and what it takes to build a strong reputation. Featuring:

- **John Gerzema**, CEO, The Harris Poll
- **Ray Day**, Vice Chair, Stagwell

To access this on-demand event replay, **please click here**.

FROM MEASUREMENT TO ACTION: NEW FINDINGS ON WORKPLACE MENTAL HEALTH

ONE MIND™ At Work

This webinar shares the initial findings from the Mental Health at Work Index, including why measurement matters, how to get a handle on what you are doing at your organization, and advice on how to advance evidence-based strategies to enhance employee mental health.

- **Kathleen Pike**, PhD, President & CEO, One Mind at Work
- **Virginia Peddicord**, Director, Global Wellbeing Resources, Bain & Co
- **Stephen Massey**, Co-Founder & Co-CEO, Meteorite
- **Sondra Davis**, CHRO, North Mississippi Health Services

To access this on-demand event replay, **please click here**.

REPLAYS FROM THE 2023 ESG FORUM

2023's ESG Forum boasted a wide range of topics and speakers sharing insights, advice, and best practices around ESG issues that ethics and compliance teams face today. Check out the replays to learn about the evolving regulatory landscape, human rights, managing and collecting ESG data, leveraging compliance to achieve ESG goals, refining your organizational workflow, working with ESG raters and rankers, and how business relationships impact ESG initiatives. Featuring:

- Navigating an Evolving Regulatory Landscape Around ESG
- Human Rights at Home: A Renewed Examination of Risks in the United States
- Removing the Data Silos: Managing & Collecting ESG Data
- Leveraging Compliance to Make Your ESG Program a Success
- Refining Your Organizational Workflow from ESG Goals to Disclosures
- Ratings & Rankings: How to Work with and Learn From ESG Raters
- Understanding & Managing Business Relationship Impacts on ESG Initiatives

To access these on-demand event replays, **please click here**.

Business Ethics Leadership Alliance (BELA)

Member Resources

BELA members receive enterprise-wide access to the BELA Member Hub—a premier repository of key resources featuring examples of work, presentations, and research provided by BELA companies, exclusive data from Ethisphere's unparalleled data set, program benchmarking, and expert reports, event sessions and other insights.

Be sure to check on the resource hub regularly to see the latest content that addresses some of the most important issues facing the ethics and compliance field today. And if you are interested in showcasing your organization and sharing a resource with the BELA Community, reach out to Manager, Content & Community Engagement, Samantha Johnson to learn more.

BELA Benefits Across Roles and Regions

We've pulled together this publication to help ensure that you and your team are making the most of all the Business Ethics Leadership Alliance (BELA) has to offer. It contains an overview of BELA resources, tools, data, events and other opportunities to improve ethics and compliance practices and programs.

Download this resource from the BELA Member Hub. Need access? Email bela@ethisphere.com

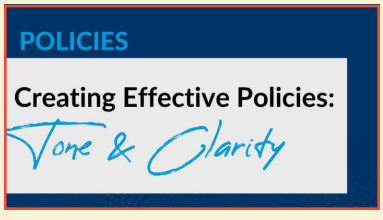
M&A Working Group Report

Data privacy has emerged as one of the most regulated and challenging compliance issues for any company. It is increasingly considered one of the most important elements in the social and governance pillars of corporate ESG. For companies and investment firms regularly focused on mergers and acquisitions, it is also an essential risk category that needs to be evaluated.

This guide, created in partnership with the BELA Compliance & Data Privacy Working Group, covers initial considerations, the pre-investment stage, collaborating with the deal team, the due diligence process, and post-investigation and integration.

Download this resource from the BELA Member Hub. Need access? Email bela@ethisphere.com.

Creating Effective Policies: Tone & Clarity



Written policies are a fundamental element of an effective compliance program and are essential for consistent communications within an organization. Policies should clearly outline expectations for behavior that is aligned with the law and the culture of the organization. The tone and clarity of your writing matters. This one-page guide shares tips and advice for crafting clear policies that guide employees in doing the right thing.

To learn more about policies and policy management, check out this resource, **Guidance for Creating a Policy on Policies**.

Download this resource from the BELA Member Hub. Need access? Email bela@ethisphere.com.

TTEC – Code of Ethics

TTEC shares their Code of Ethics that covers, among other things, ethical decision making, appropriate workplace conduct, conducting business ethically, compliance with laws and regulations, and TTEC's responsibility to their shareholders.

The Code was recently updated to include expanded governance standards for the ethical use of artificial intelligence in their business.

Additionally, TTEC shares an example of the categories available to reporters utilizing their We Hear You Helpline (the ethics and compliance hotline), which includes a recent addition of a standalone AI category for improved tracking and management of AI-related concerns.

Download this resource from the BELA Member Hub. Need access? Email bela@ethisphere.com.

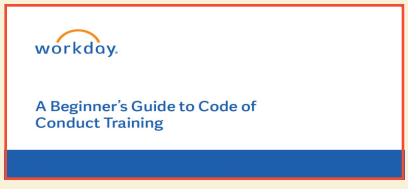
Corporate Responsibility & Compliance Board Charter

AMGEN®

Amgen shares their charter for their Board committee on Corporate Responsibility and Compliance. It covers membership on the committee, meetings and procedures, and member responsibilities.

Download this resource from the BELA Member Hub. Need access? Email bela@ethisphere.com.

A Beginner's Guide to Code of Conduct Training



Workday shares this guide to Code of Conduct training that covers assessing your current training, what topics should be covered, the training experience, and engaging with the organization.

Download this resource from the BELA Member Hub. Need access? Email bela@ethisphere.com.

BELA Asks Series Recap

Last year, the Ethicast published a series of BELA Asks episodes that addressed questions posed by members of the Business Ethics Leadership Alliance about wider issues facing the ethics and compliance community. The series was a huge hit and new episodes are being published now. But in the meantime, here are our first series of episodes for those who wish to get caught up.

- How Many Fortune 500 Companies List Their Values on Their Websites?
- How Do I Create and Refresh My Ethics and Compliance Policies?
- What Goes Into a Good Multi-Year Compliance Plan?
- How Do I Train My Board?
- How Many Investigations Is Ideal?
- What Should We Do with Investigations Data?
- How Do We Close an Investigation?

Download this resource from the BELA Member Hub. Need access? Email bela@ethisphere.com.

Applying AI Responsibly

Establishing Ethical Values for a Transformative Technology

by Justin Newell

The rapid rise and spread of artificial intelligence (AI) demands that we don't just use it with good intentions, but that we craft Responsible AI guidelines and then live by them.

You can't pick up a newspaper or magazine without seeing the initials AI. Artificial Intelligence (AI) is dominating headlines and corporate boardrooms alike. Its proliferation is undeniable. Expectations are that this groundbreaking technology—the roots of which date back to the mid-1950s with "The Logic Theorist" program funded by Research and Development (RAND) and presented at the "Dartmouth Summer Research Project on Artificial Intelligence"—will continue to grow and permeate almost all aspects of society.

MarketsandMarkets projected the AI market to reach $407 billion by 2027, and Statista reported that it will have an estimated 21% net increase on the United States' gross domestic product (GDP) by 2030. For AI vendors, that's all good news. AI does have great promise to deliver many benefits. It is already driving automation and increased productivity, enhancing customer service, supporting medical research, enabling autonomous vehicles, creating consumer-generated advertising, providing greater data protection and cybersecurity, and much more.

There is, however, broad concern about its misuse and abuse. In the wrong hands, AI can lead to a host of cybercrimes that can cripple critical infrastructure, drive financial fraud, invade privacy, and even generate a new medical crisis. While we can't completely stop the bad guys, we can take measures that support promote responsible and ethical use of AI. At the top of that list is understanding the AI landscape today, how best to leverage AI, and why responsible AI guidelines are critical.

THE AI LANDSCAPE

AI applications are growing rapidly, but we've only tapped the surface of their potential. Back in 2017, The Boston Consulting Group found that 85% of executives believed AI would give their companies a competitive edge. Then, just one in five executives had incorporated AI into their offerings. An April 2023 *Forbes Advisor* survey found that 73% of businesses use or plan to use AI. Those numbers surely have not remained static since.

Among the trends driving AI adoption is the current labor shortage. The *IBM Global AI Adoption Index 2022* noted that 25% of companies are looking to AI to address their workforce challenges and, on the flip side, many workers cite concern over AI replacing their jobs. It's not a concern without merit as The McKinsey Global Institute reports that 400 million workers could conceivably be displaced by AI. Those opposed to this thinking cite what humans have that AI doesn't: common-sense reasoning, the ability to collaborate with other humans, natural language understanding, empathy, etc. Additionally, it is more likely that AI will create new job opportunities which the World Economic Forum said could be as high as 97 million new jobs.

Currently, AI is delivering many benefits in streamlining manufacturing, supply chain processes, medical research, advertising, and hospitality processes. It's speeding up production lines, supporting supply chain digitalization and resilience, responding to consumers' financial inquiries, developing new therapies and improving patient outcomes, creating social media posts, and planning travel itineraries.

AI CHALLENGES

Its abuse in the hands of criminals notwithstanding, there are other common challenges facing AI. As previously noted, there is a lack of AI talent. Many businesses do not have staff with the expertise in AI technologies and how best to integrate and apply them. They are also unaware of how their customers will react and interact with AI.

Another challenge lies in the area of data privacy, security and related data breaches and dark web implications. Similarly, there are challenges relating to restricting the flow of data to prevent its unethical use which can potentially taint the accuracy of AI-generated results. Also relating to data is the issue concerning its capture and storage. AI systems use sensor data which can be massive but essential to validate AI findings. When these massive sets of data become difficult to store and assess, they can hinder AI's algorithms and cause poor results.

Additionally, system-related issues pose a challenge. AI, Machine Learning and Deep Learning require considerable computing power for algorithms to perform. The power

required is almost equivalent to that of a supercomputer which comes with a high price tag. Cloud computing and parallel processing are somewhat of a remedy, but not always sufficient to support the large amounts of data and complex algorithms AI uses.

While these challenges are significant, the ethical and legal challenges AI poses require the most thought and strategy on the part of AI adopters and providers.

ETHICAL AI

Despite its challenges and the many alarmist headlines, AI has the potential for the greater good across many sectors of our lives. The key to harnessing its power for the greater good is its ethical application reflecting responsible guidelines, best practices, and an ethical foundation. At the core of these requirements are pivotal principles that align with and drive trustworthy AI. Following are those principles:

- **Beneficial AI.** Ensuring AI systems enrich both users and society, mitigating negative impacts on society and businesses such as bias amplification, misinformation, and societal divides.
- **Human-centric.** Promoting AI's supportive role to humans, assisting them in their work, enhancing decision-making processes and upholding human responsibility. It requires the review of AI algorithm outputs prior to results being put into practice. In cases of real-time decision-making, it's important to allow for human monitoring and auditing thereby keeping accountability with humans and not an autonomous agent.
- **Aligned AI.** Guaranteeing AI is in sync with human and business values with clear and understandable AI as a foundation. Reflecting human and business objectives should be an integral part of continuous AI algorithm engineering. This facilitates the control of judgements to determine what a "good solution" represents in, for example, objective function in machine learning and training data's analysis for bias.
- **Privacy-preserving AI.** Upholding the European Union's GDPR standards and achieving top-tier security standards endorsed by ISO 27001 certifications. The goal is to adhere to all relevant legislation, while being mindful of data protection and the ethical use of AI for use cases that significantly affect people.
- **Reliable AI.** Prioritizing quality consistency and transparency in AI applications, especially in vital sectors. This requires the use of good software engineering practices for the design, development and testing of algorithms. Where machine learning algorithms are concerned, it is especially important that training data be thoroughly analyzed for bias with testing focused on unreasonable or other unwanted results. In operation, AI-based software audit trails and other software capabilities further provide monitoring to ensure reliability under changing conditions.
- **Safe AI.** Crafting AI algorithms that ensure safety and ward off potential threats. This requires that their impact be clearly confined to a business' domain in which the algorithms operate, and clearly defined interfaces surrounding the domain. This is routinely provided for search and optimization algorithms, as well as for focused AI use cases. In situations involving Large-Language Models using similar AI logic and for which safety issues can arise, best practices call for impact containment. If containment to the business domain is not evident, then the AI system should be subjected to an internal review to identify potential impacts (e.g., malicious API calls, code injection, jailbreaking and other malicious practices).

The intent of these principles is to maximize AI's potential while minimizing risks. Trustworthy AI can only be achieved when society's needs, and individual rights are prioritized.

Putting aside the hype and the naysayers, AI is a powerful, transformative tool that will continue to have enormous impact on our personal and professional lives. It has already demonstrated enormous value when channeled through best practices and responsible use. Building trust in AI's broader application requires a commitment to sound principles that help mitigate potential risks and foster maximum benefits. Responsible AI conduct backed by ethical values is an essential prerequisite. ■

ABOUT THE AUTHOR

Justin Newell *is Chief Executive Officer of INFORM North America, a leading provider of AI-based optimization software that facilitates improved decision making, processes and resource management, and a member of the INFORM Group, a global organization headquartered in Aachen, Germany. INFORM has published its Responsible AI Guidelines, the pillars of which are the six guiding principles which are noted in this article.*

Six Ethical Artificial Intelligence Principles for Your Code of Conduct

by Susan Jones

Ethical AI does no harm. But for it to live up to its considerable potential and avoid its much-discussed pitfalls, then it needs human oversight.

In a recent Pew Research article, Rainie et al wrote that artificial Intelligence (AI) applications "speak" to people and answer questions. They run the chatbots that handle customer-service issues. They help diagnose cancer and other medical conditions. They scour the use of credit cards for signs of fraud and determine who could be a credit risk. They are the operating system of driverless vehicles. They sift applications to make recommendations about job candidates. They determine material that is offered up in people's newsfeeds and video choices. They recognize people's faces, translate languages and suggest how to complete people's sentences or search queries. They can "read" people's emotions. They beat them at sophisticated games. They write news stories, paint in the style of Vincent Van Gogh and create music.[1]

Artificial intelligence systems are spurring headlines with new breakthroughs, all the while fostering worries about job skills, workforce replacement, burgeoning use without appropriate or regulated oversight, and potential bad actors. Even world leaders are working to reap the benefits of AI while strategizing how to keep various risks at bay. Last October, it was announced that the "G7 (a group of seven industrial countries consisting of Canada, France, Germany, Italy, Japan, Britain, and the United States) along with the European Union, will develop an 11-point Code of Conduct around AI worldwide that is meant to help seize the benefits and address the risks and challenges brought by these technologies".[2]

With so many AI uses at hand, a primary focus now is ensuring the use of ethical AI. What exactly, is ethical AI? "Ethical AI is artificial intelligence that adheres to well-defined ethical guidelines regarding fundamental values, including such areas as individual rights, privacy, non-discrimination, and non-manipulation. Ethical AI places fundamental importance on ethical considerations in determining legitimate and illegitimate uses of AI."[3]

Here is where the Code of Conduct steps forward as a key educational platform for applying ethical AI. This article discusses six key principles addressing ethical AI within a Code of Conduct, beginning with an overarching principle regarding organizational alignment, oversight of the adoption of AI, and the establishment of a roadmap to manage identified functional risks associated with the use of AI. The remaining principles focus on the user of AI, the individual sharing data with an AI system—with the expectation of an improved product, a problem-solving solution, or the efficient completion of a task in an attempt to work smarter not harder. Ethical AI principles within your Code of Conduct strive to mitigate risk at the first stop in the journey—the user—and can serve as a living set of principles that evolve alongside the development of AI.

Here are the six key principles addressing ethical AI within a Code of Conduct.

1. Establish an AI Governance Council

Why is this needed? Provides organizational alignment, oversight of the adoption of AI, and addresses mitigation of risk.

In order to ensure enterprise-wide alignment on the adoption and safe use of AI, establish an AI Governance Council. Obtain appropriate executive sponsorship from the Chief Compliance Officer and/or the Chief Information Officer to support initiatives. Outline the primary responsibilities and accountabilities for the AI Governance Council and set forth a roadmap for the company to ensure the adoption of ethical AI is implemented in a controlled and responsible manner that mitigates risk for the workforce and the company as a whole.

2. Protect Company Data

Why is this needed? Aims to protect intellectual property by preventing inappropriate sharing with AI.

As Markel et al wrote, not all AI systems are alike. "Open" AI systems (those that do not limit how the prompts input to the system are used by the AI tool), such as ChatGPT, Bard, and other AI chatbots are free and available to all users inside and outside the workplace. Information that is entered into an "open" AI system might be shared with another unintended user, and retained in the AI's neural network, potentially in perpetuity, to be used for further training of the system.[4] This data is now untethered, likely unretrievable, and becomes part of the AI lexicon available to all other

users, leaving the employer without control over how the data is to be used or with whom it might be shared.

"Unlike 'open' AI systems, 'closed' AI systems are typically proprietary and may limit or prevent circumstances under which user prompts would be shared with outside users."[4] However, these systems still require an understanding of how and when information entered into the system could be shared outside of the intended recipients.

Assurance activities such as training the workforce on all relevant company policies, standard operating procedures, and information classification and records management protocols should be in place at the outset to prevent the inadvertent sharing of sensitive or confidential information with AI applications. Managerial review and approval of intellectual data should occur in advance of any plans to utilize AI in order to detect issues before they become public news. Provide clearly defined procedures on the appropriate and compliant use of AI and ensure support systems are in place to assist users with AI technology. Protecting the company's intellectual property, reputation, and trustworthiness is a top priority.

3. Safeguard Individual Privacy

Why is this needed? Aims to prevent violations of privacy law and associated civil or monetary penalties.

Artificial intelligence systems collect vast amounts of information that may include personal information such as names, addresses, biometrics, preferences, and financial and medical records, to name a few. Cybersecurity hacks and data breaches create damaging news headlines, expose organizations to legal and regulatory risk, and alarm individuals about potential identity theft, financial risk, medical data exposure, and other malicious uses of personal data.

In the United States, privacy laws exist at both the federal and state levels. Federal laws such as the Gramm-Leach-Bliley Act (GLBA) which protects financial privacy or the Health Insurance Portability and Accountability Act (HIPAA) which protects patient health information, are sector-specific to that particular industry. On the other hand, AI systems touch a multitude of industries and it is the Federal Trade Commission (FTC) that occupies a strategic position with the needed tools and authority (derived from the FTC Act) to protect the consumer from deceptive or unfair practices, including infringements on privacy, associated with AI. Additionally, state and local levels of government may have current or proposed AI frameworks for addressing individual privacy as well.

"Appropriate oversight of AI-generated materials should include the assessment of any potential bias, discrimination, inaccuracy or misuse."

Taking steps to safeguard personal data from unauthorized access and wrongful use is not only essential, but critical. Respect personal privacy by adhering to applicable federal and state privacy laws. Create and implement a privacy impact assessment for use prior to inputting any data into an AI tool. Train the workforce on required disclosures and requirements for obtaining consent from individuals prior to collecting sensitive personal information such as financial or health data. Provide training on relevant policies and procedures, appropriate security measures, and how to report a privacy incident.

4. Promote Appropriate and Respectful Use of AI

Why is this needed? Promotes ethical AI use through effective training and identifies resources for voicing concerns or reporting behavior related to unethical use of AI.

Training should include emphasis on the use of AI in a respectful and professional manner at all times. Only company-approved AI tools should be utilized. Avoid use of profanity and any form of indecent or discriminatory language. Avoid use of any communication that may be perceived as offensive. Review established avenues for voicing concerns or reporting behavior related to unethical use of AI.

5. Prevent Incorporation of Bias, Discrimination, Inaccuracy, and Misuse

Why is this needed? Supports requisite fairness when evaluating AI input and output.

"For a machine to 'learn', it needs data to learn from, or train on. Examples of training data are text, images, videos, numbers, and computer code," notes a 2023 Reuters article on AI and employee privacy. "In most cases, the larger the data set, the better the AI will perform. But no data set is perfectly objective; each comes with baked-in biases, or assumptions and preferences."[5]

A 2023 Harvard Business Review article goes even further: "Bias can creep into algorithms in several ways. AI systems learn to make decisions based on training data, which can include biased human decisions or reflect historical or social inequities, even if sensitive variables such as gender, race, or sexual orientation are removed. Amazon stopped using a hiring algorithm after finding it favored applicants based on words like 'executed' or 'captured'

that were more commonly found on men's resumes, for example."[6]

Generative AI can produce inaccurate or false information referred to as "hallucinations" and present it as if it were fact. These nonsensical or inaccurate results can arise from limitations or biases within algorithms, insufficient or low-quality data sets, or a lack of appropriate context, for example. Glover wrote, AI hallucinations are a direct result of large language models (LLMs) which are what allow generative AI tools (like ChatGPT and Bard) to process language in a human-like way. Although LLMs are designed to produce fluent and coherent text, they have no understanding of the underlying reality that they are describing. All they do is predict what the next word will be based on probability, not accuracy.[7] If you needed a reason to double check the output of AI, this is it. Failure to verify the accuracy of AI output risks providing inaccurate, fabricated, or even dangerous information.

Misuse is another area of caution. "Organizations can improperly use licensed content through generative AI by unknowingly engaging in activities such as plagiarism, unauthorized adaptations, commercial use without licensing, and misusing open-source content, exposing themselves to potential legal consequences."[8]

Establish processes to recognize and address such issues. Do not take AI output at face value. Question it, evaluate it, look for transparency in how the algorithm produced it, have an appropriately qualified human double-check it, and implement an assessment form to identify red flags for further investigation. Provide on-going training and development to the workforce to reinforce the responsible use of AI tools.

6. Ensure Accountability, Responsibility, and Transparency

Why is this needed? Emphasizes responsibility and promotes an auditable and traceable process.

It is important that anyone choosing to apply AI to a process or data for example, must have sufficient knowledge about the subject. The user is responsible for identifying whether data is sensitive, proprietary, confidential, or restricted beforehand and should consult with management regarding the decision to apply AI to the process. The end-to-end process for using AI needs to be transparent. Ideally, the user should advise the recipient that AI was used to generate the data, identify the AI system employed, explain how the data was processed, and communicate limitations that may apply.

Review all data generated by AI for accuracy prior to its use and/or distribution. Appropriate oversight of AI-generated materials should include the assessment of any potential bias, discrimination, inaccuracy or misuse. The data produced should be auditable and traceable throughout its lifecycle development.

The application of ethical AI needs human oversight. Ethical AI does no harm. It aims to protect intellectual property, safeguard privacy, promote appropriate and respectful use, prevent incorporation of bias, discrimination, and inaccuracy, and ensure accountability, responsibility, and transparency. These are all praiseworthy attributes that fit squarely into Code of Conduct. ■

ENDNOTES

1. *Rainie, Lee; Anderson, Janna; Vogels, Emily A. Experts Doubt Ethical AI Design Will Be Broadly Adopted as the Norm Within the Next Decade. Pew Research Center Page. Retrieved November 22, 2023, from https://www.pewresearch.org/internet/2021/06/16/experts-doubt-ethical-ai-design-will-be-broadly-adopted-as-the-norm-within-the-next-decade/.*

2. *Chee, Foo Yun. Exclusive: G7 to agree to AI code of conduct for companies. Reuters Page. Retrieved November 22, 2023, from https://www.reuters.com/technology/g7-agree-ai-code-conduct-companies-g7-document-2023-10-29/.*

3. *Glossary Ethical AI. C3ai Page. Retrieved November 27, 2023, from https://c3.ai/glossary/artificial-intelligence/ethical-ai/.*

4. *Markel, Keith A.; Mildner, Alana R.; Lipson Jessica L. AI and employee privacy: important considerations for employers. Reuters Page. Retrieved November 29, 2023, from https://www.reuters.com/legal/legalindustry/ai-employee-privacy-important-considerations-employers-2023-09-29/.*

5. *California Institute of Technology Faculty. Can We Trust Artificial Intelligence? California Institute of Technology Science Exchange Page. Retrieved November 29, 2023, from https://scienceexchange.caltech.edu/topics/artificial-intelligence-research/trustworthy-ai.*

6. *Manyika, James; Silberg, Jake; Presten, Brittany. What Do We Do About the Biases in AI? Harvard Business Review Page. Retrieved November 27, 2023, from https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai.*

7. *Glover, Ellen. What Is An AI Hallucination? Built In Page. Retrieved November 30, 2023, from https://builtin.com/artificial-intelligence/ai-hallucination.*

8. *Spisak, Brian; Rosenberg, Louis B.; Beilby, Max.13 Principles for Using AI Responsibly. Harvard Business Review Page. Retrieved November 27, 2023, from https://hbr.org/2023/06/13-principles-for-using-ai-responsibly.*

ABOUT THE AUTHOR

Susan Jones *is a Senior Manager at Amgen Inc., in the Worldwide Compliance & Business Ethics function. With 25+ years of experience, Susan has worked in highly cross-matrixed environments, building and leading teams, developing training resources, and supporting compliant and ethical business initiatives. While she has a connection to Amgen, opinions are her own and do not represent Amgen's position.*

HUSCH BLACKWELL

Uncommon For Good Reason

Husch Blackwell is a different kind of law firm. One where trailblazing leadership and inventive approaches deliver unmatched personal service and guidance, helping you assess risk and protect both your reputation and your business.

Our team is well-versed and highly experienced in compliance and government enforcement, enabling us to develop comprehensive compliance programs and conduct internal investigations that can detect and prevent misconduct before it leads to government intervention. When prosecution does occur, we work to secure the best possible outcome, either through settlement or vigorous trial defense.

When the AI Does It, Does That Mean It Is Not Illegal?

Navigating an "Existing Authorities" Regime for AI Regulation

by Michael Martinich-Sauter and Rebecca Furdek

As artificial intelligence (AI) proliferates, so do its legal complications, forcing companies to know the risks and rewards of abiding by AI regulatory expectations as they currently exist in a world where they will surely not stay that way for much longer.

Artificial intelligence (AI) seems to be everywhere you look these days. The launch of OpenAI's Chat GPT-3 and GPT-4 dominated media headlines. So too have concerns about potential harms caused by AI, ranging from misinformation, to job displacement, to the potential extinction of humanity. Despite these concerns, AI only grows more ubiquitous in daily life. AI chatbots help us buy products online, AI facial recognition helps us get through airport security, and AI applications help doctors diagnose our ailments.

The pervasiveness, potential, and perceived risk of AI are not lost on Congress. Both the House and Senate held hearings on AI in 2023, and legislators introduced a flurry of AI-related bills. To date, however, Congress has not enacted comprehensive AI legislation. The absence of express legislative authority has not deterred regulators from seeking to rein in AI, though. In doing so, these agencies have focused on using their existing authority to regulate the new challenge of AI. As the Federal Trade Commission (FTC) put it, there is "no AI exemption from the laws on the books."[i] This reliance on existing legal authorities and enforcement frameworks tracks how federal agencies have often approached cybersecurity regulation. In the absence of comprehensive federal cybersecurity legislation, a key component of the White House's National Cybersecurity Strategy involves using "existing authorities to set necessary cybersecurity requirements."[ii]

As companies evaluate their AI-related risk, then, they cannot simply look to the latest AI-related legislation or regulation. So where should compliance and legal teams focus as they navigate an "existing authorities" approach to regulating AI? Below are several relevant guideposts to consider when evaluating AI-related regulatory risk.

OUTCOME-BASED VS. INTENT-BASED REGULATION

As companies evaluate their relative regulatory risk, one potentially relevant factor is whether liability under the applicable regulatory scheme depends on a party's intent or knowledge. AI systems notoriously have the potential to take action that their creators neither intended nor anticipated. In one recent example, researchers found that an AI application would engage in insider trading, even when specifically instructed not to do so.[iii]

These unintended consequences can create significant regulatory risk where the relevant statute or regulation imposes liability on outcomes rather than intent. For instance, a company can violate the federal Fair Housing Act and its implementing regulations if its business practices cause a disparate impact on a protected class, even if that effect was entirely unintended.[iv] Thus, if a landlord uses an AI system to screen prospective tenants and that system disproportionately disfavors minority applicants, the landlord may face significant regulatory risk even if he or she had no discriminatory intent. Some other regulatory regimes require that a party possess certain intent or knowledge before imposing liability. For example, establishing fraud ordinarily requires showing that a party possessed fraudulent intent.

When assessing whether or how to incorporate AI into your operations, being mindful of the distinction between outcome-based and intent-based regulation can help assess the relative risk your company may face. It also points toward potential ways to mitigate that risk. Companies should consider carefully documenting the business rationale for adopting AI systems, the steps taken to avoid adverse consequences, and the reasons why less risky options are not practical. Where the applicable regulations focus on intent, this contemporaneous documentation can help establish that the company lacked an impermissible intent. It may also help prevent regulators from trying to prove intent by characterizing the company as recklessly disregarding known risks.

Even when regulations focus on outcomes rather than intent, documenting the company's motives and good-faith efforts to avoid harm can heavily impact a regulator's prosecutorial discretion. In addition, some outcome-based regulatory regimes provide narrow defenses based on good faith or business necessity. For example, the federal fair-housing regulation discussed above permits a defendant to justify a business practice on the ground that the practice achieved a legitimate, nondiscriminatory purpose and that no less discriminatory alternative

would suffice. Documenting the business purpose and the insufficiency of alternatives can provide critical evidence for a company that will later rely on such a defense. In some cases, the exercise of documenting these considerations can also help identify previously overlooked alternative options that can mitigate regulatory risk and even enhance business outcomes.

DISCLOSURE REGARDING THE USE AND OPERATION OF AI

While some regulators are on uncertain footing when using their existing authorities to regulate AI, agencies like the FTC and state attorneys general possess an expansive and well-established tool: statutory authority to challenge "unfair or deceptive acts or practices."[v] It should come as no surprise, then, that the FTC has taken a leading role in attempts to police AI, with a particular focus on how companies market or disclose their use of AI.

The most obvious area of FTC focus is where a company deceptively overhypes its AI. As the FTC succinctly puts it: "Keep your AI claims in check."[vi] But there can also be risk from saying *too little* about your use of AI. Material omissions can sometimes deceive just as much as false statements. For example, there may be scenarios where AI-generated content is so true-to-life that the failure to disclose its AI origins is deceptive.[vii] Similarly, the FTC contends that "people should know if they're communicating with a real person or a machine."[viii] Companies should expect the FTC to closely scrutinize chatbots and similar features used in persuading consumers to buy goods or services.

The FTC's enforcement approach forces companies to navigate between Scylla and Charybdis: say too much about your AI and risk the perception that you've mischaracterized it; say too little and risk the perception that you've left out something material. Further complicating the task, an AI system's internal operations often remain opaque even to its creators. There is no easy solution to this predicament. Compliance teams must work closely with technical and marketing staff to understand how AI works "under the hood," as well as the intended and foreseeable ways that consumers might interact with it.

USING TOO LITTLE AI

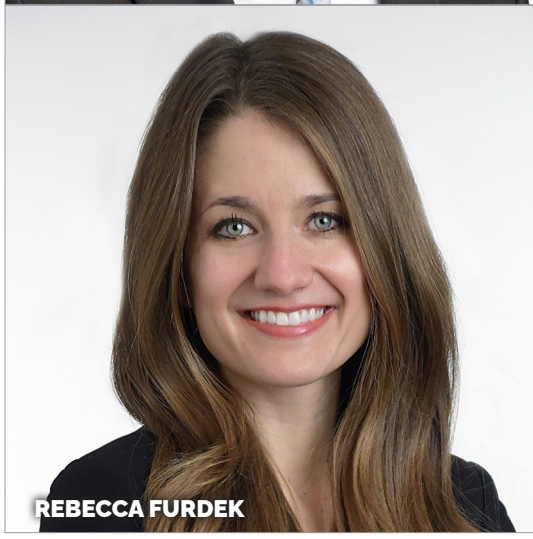
When thinking about AI-related risks, we often focus on the risks that come from using AI. But in some cases, *failing* to use AI may also bring regulatory risk. As AI becomes more pervasive in business given its many potential benefits, the government likely will come to expect companies to incorporate AI into their compliance and know-your-customer programs.

In some cases, where other regulatory regimes impose an affirmative obligation to identify potential risks, the government might view the absence of AI in these functions as undermining the adequacy of the company's program. For example, the FTC's financial-institution cybersecurity regulations require regular penetration testing and monitoring for cyber vulnerabilities.[ix] Identifying such vulnerabilities is a well-recognized use case for AI. For this reason, the FTC may soon expect that any effective penetration-testing and vulnerability-monitoring regime will include AI, and the failure to use AI may constitute a violation of the relevant regulations. As a result, companies should continually consider how AI developments can enhance their non-AI compliance and risk-management efforts. ■

ENDNOTES

i. *FTC Comment to Copyright Office Docket No. 2023-6, Artificial Intelligence and Copyright, Fed. Trade Comm'n, at 8 (Oct. 30, 2023)*
ii. *National Cybersecurity Strategy, White House at 8 (March 2023)*
iii. *Matt Levine, The Robots Will Insider Trade, Bloomberg Law News (Nov. 11, 2023)*
iv. *24 C.F.R. § 100.500*
v. *15 U.S.C. § 45*
vi. *Michael Atleson, Keep your AI claims in check, Fed. Trade Comm'n (Feb. 27, 2023)*
vii. *Michael Atleson, Chatbots, deepfakes, and voice clones: AI deception for sale, Fed. Trade Comm'n (Mar. 20, 2023)*
viii. *Michael Atleson, The Luring Test: AI and the engineering of consumer trust, Fed. Trade Comm'n (May 1, 2023)*
ix. *16 C.F.R. § 314.4(d)*


MICHAEL MARTINICH-SAUTER


REBECCA FURDEK

ABOUT THE AUTHORS

Michael Martinich-Sauter *is a partner in the St. Louis office of Husch Blackwell LLP. He regularly represents innovative companies in government investigations and regulatory compliance matters.*

Rebecca Furdek *is a senior associate in the Milwaukee office of Husch Blackwell LLP. She represents individual and corporate clients in both civil litigation and defending against government investigations.*

National Security and Government Contractor Implications of Biden AI Executive Order

Understanding the Biden Administration's First Robust Attempt to Shape the Development of the Emerging AI Industry

by Tina D. Reynolds, Charles L. Capito, Brandon L. Van Grack, and Lyle F. Hedgecock

At the end of October 2023, the Biden administration issued a widely anticipated executive order on artificial intelligence (AI). The Executive Order on the Safe, Secure, and Trustworthy Development of Artificial Intelligence (the EO) addresses a multitude of issues reflecting an emerging national policy on AI.

NATIONAL SECURITY CONSIDERATIONS

Generative and other emerging AI applications have myriad implications for U.S. national and global security. To address the multitude of issues reflecting an emerging national policy on AI, the Biden administration issued a widely anticipated executive order on artificial intelligence (AI) at the end of October 2023.

First, the EO requires that developers of the most powerful AI systems, so-called "dual-use foundational models," conduct and report the results of safety testing, and share other critical information with the federal government. These foundational models implicate national security, economic security, and public health and safety. Companies will also be required to report planned activities in training dual-use AI, developing or producing such systems, and to outline the precautions they are taking during the development process.

The administration invokes the Defense Production Act as the authority for compelling disclosure of this information, much of which will be proprietary. Although several leading AI companies already share such information voluntarily, this provision seeks greater disclosure regarding companies' deployment of AI and the testing and risk assessments underpinning AI models.

This disclosure requirement is related to one of the EO's many agency directives. Specifically, the EO directs the National Institute of Standards and Technology (NIST) to develop standards to verify that AI systems are safe, secure, and trustworthy, in the form of companion guidance to already-existing NIST publications, such as the AI Risk Management Framework (NIST AI 100-1).

Second, the EO calls for regulations to require U.S. Infrastructure as a Service (IaaS) providers to report transactions with foreign persons to train large AI models with potential capabilities that could be used in malicious cyber activity. The forthcoming regulations will also require IaaS providers to prohibit foreign resellers from providing services unless they provide details about the end users, end uses, and the underlying applications.

This requirement addresses similar concerns that the Department of Commerce flagged in its October 17, 2023 advanced semiconductor rules concerning cloud-based access to advanced computing and AI training models.

Finally, the EO recognizes the potential for misuse of AI in a manner that might allow non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons. As such, the EO directs the Department of Homeland Security, in consultation with the Department of Energy and the Office of Science and Technology Policy,

private AI laboratories, and academia, to evaluate CBRN threats from AI models and develop means to mitigate these risks. Various government agencies are also directed to consider what government data might present security risks with respect to CBRN weapons and to ensure that such data is restricted from public access and not used to train AI systems.

FEDERAL PROCUREMENT CONSIDERATIONS

The EO also includes numerous developments and takeaways for government contractors, as the administration, as it often does, leverages its purchasing power to effect policy goals.

First, the EO provides guidance for the procurement of AI products and services by federal agencies. The EO directs the Office of Management and Budget (OMB) to specify minimum risk-management practices for governmental use of AI. These requirements include:

- establishing a Chief Artificial Intelligence Officer (CAIO) charged with AI implementation in the agency;
- defining the CAIO's roles and responsibilities;
- requiring certain agencies to create an AI governance board;
- implementing minimum risk management practices;
- identifying AI uses that impact individual rights or safety;
- recommending ways to reduce barriers to AI use;
- requiring certain agencies to develop AI strategies and pursue advantageous use of AI;
- external AI testing for generative AI, safeguards preventing discriminatory use or other misuse of AI, watermarking, minimum risk management practices, independent assessment of vendor effectiveness and risk mitigation claims, documentation and oversight of AI, maximizing value of contracted AI services, and incentivizing continuous improvement of AI;
- training agency employees on AI; and
- public reporting on compliance with these requirements.

Additionally, OMB is tasked with requiring that agencies make sure that any contracts for AI services address: privacy, civil rights, and civil liberty concerns; ownership and security of data; and means to prevent misuse, unauthorized use, or corruption of AI systems.

Second, Section 4.5(d) of the EO directs the Federal Acquisition Regulatory Council to consider amending the Federal Acquisition Regulation (FAR) to reduce risks posed by "synthetic content" and to require identification of synthetic content produced by AI systems used by the federal government or on its behalf. The aim is to promote trust in the integrity and authenticity of U.S. government digital content by establishing transparency regarding the provenance of generated content and preventing generation of inappropriate or inaccurate content.

Third, in line with this goal, the EO directs the Secretary of Commerce (in consultation with other agencies) to develop standards, tools, methods, and practices for use by federal government agencies and contractors: (1) to authenticate and track the provenance of AI-generated material; (2) to label AI content using methods such as "watermarking"; (3) to detect synthetic content; (4) to prevent AI from producing certain abusive, explicit materials, such as nonconsensual, AI-generated representations of real people (i.e., "deepfakes"); to (5) test; and (6) audit software for these purposes.

Pending release of this guidance, agencies seeking to obtain AI products or services are required to implement "minimum risk-management practices" defined in Section 10.1(b)(iv). These practices are derived from the


TINA D. REYNOLDS


CHARLES L. CAPITO


BRANDON L. VAN GRACK


LYLE F. HEDGECOCK

White House Office of Science and Technology Policy's Blueprint for an AI Bill of Rights and the NIST AI Risk Management Framework, and they include: (1) public consultation; (2) review of data quality; (3) assessing and mitigating discriminatory impacts from AI; (4) providing notice when an agency employs AI; (5) continuously monitoring and evaluating AI in use; and (6) granting separate, "human" consideration and remedies for adverse decisions made by AI systems.

Section 7.2 also requires agencies to "use their respective civil rights and civil liberties offices and authorities…to prevent and address unlawful discrimination and other harms that result from uses of AI in Federal Government programs and benefits administration."

Finally, beyond the directives and proposed regulatory requirements, the EO suggests business opportunities for potential recipients of federal grant and contract funding. It directs the General Services Administration to facilitate government-wide acquisition solutions for AI services and products, thereby creating future consolidated contracting opportunities to provide AI tools to the federal government.

Specifically, the EO encourages acceleration of grants awarded through the National Institutes of Health Artificial Intelligence/Machine Learning Consortium to Advance Health Equity and Researcher Diversity program and through the Advanced Research Projects Agency-Infrastructure (ARPA-I) to explore transportation-related opportunities and challenges of AI, including regarding software-defined AI enhancements impacting autonomous mobility ecosystems.

The EO also proposes a pilot project to "identify, develop, test, evaluate, and deploy AI capabilities, such as large-language models, to aid in the discovery and remediation of vulnerabilities in critical United States Government software, systems, and networks." It also seeks to promote competition and innovation in the semiconductor industry, by working in concert with the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022 to use AI in the industry and provide other assistance, particularly for small businesses, and to share data for CHIPS research and development programs.

NEXT STEPS AND FINAL THOUGHTS

The EO requires implementation in the form of agency-issued guidance and potential legislation to effectuate some of its more ambitious aspects. Given the EO's tight deadlines, in the coming months we expect to see new agency-level AI policies, as well as requests for information and requests for comments on proposed rules.

IaaS providers and developers of "dual-use" AI should anticipate a roll out of reporting requirements and requests for information. Similarly, government contractors should expect that reporting regarding their AI models may become part of the proposal evaluation and embedded as contract requirements, particularly as it relates to safety of AI products, routine testing for bias, and data security and privacy protections. Contractors should also anticipate requirements for AI transparency and provenance to become a feature in government AI procurement.

Although many of the policy details are still under development, the EO represents the Biden administration's first robust attempt to shape development of the AI industry. ■

For additional articles on this Executive Order, visit the Morrison Foerster AI Resource Center, where this article was originally published.

ABOUT THE AUTHORS

Tina D. Reynolds *is co-chair of Morrison Foerster's Government Contracts & Public Procurement practice. She counsels a wide variety of government contractors on compliance with federal acquisition and ethics regulations. She drafts and negotiates contracts on their behalf and has been involved with numerous internal investigations and compliance reviews, and with bid protest, contract claims, and False Claims Act litigation. She also advises on M&A transactions involving government contractors.*

Charles L. Capito *is a partner in both Morrison Foerster's National Security and Government Contracts + Public Procurement practices. In the National Security space, he has significant experience counseling clients on the complex and evolving considerations related to the Committee on Foreign Investment in the United States (CFIUS). Charles frequently helps investors and U.S. businesses through every aspect of the CFIUS process, from understanding and allocating CFIUS risk.*

Brandon L. Van Grack *co-chairs Morrison Foerster's National Security and Global Risk + Crisis Management groups. His practice focuses on investigations, criminal defense, and compliance matters involving sanctions and export controls, foreign investment, and cyber incidents. Brandon's arrival to Morrison Foerster follows more than a decade of service at the U.S. Department of Justice (DOJ), where he held multiple senior national security positions.*

Lyle F. Hedgecock *is an associate in the Government Contracts practice group in the Washington, D.C. office. Prior to joining Morrison & Foerster, Lyle served as a law clerk at the U.S. Court of Federal Claims and had a decorated military career in the U.S. Air Force. Following his active-duty service, he provided legal services to the Air Force Legal Office, Joint Base Andrews, to resolve high-profile white-collar investigations of suspected Federal Acquisition Regulation violations and counseled government clients on Federal Acquisition Regulation compliance issues.*

APRIL 22-24, 2024

A HYBRID EXPERIENCE

ATTENDGES.COM

AGENDA NOW LIVE

2000
PARTICIPANTS

90
INDUSTRIES

100
SPEAKERS

350
ORGANIZATIONS

WHERE ETHICS AND COMPLIANCE INNOVATORS COME TO *Grow*

REGISTER TODAY

Don't wait, take advantage of a **20% discount** to join the premier Ethics, Compliance and ESG community gathering.

use discount code: ***MAG24***

ATTENDGES.COM

SIGNIA BY HILTON ATLANTA, GA | VIRTUAL

From Data to Decisions

Emergence of Generative AI as a Game-Changer in Supply Chain Risk Management

by Craig Moss and Vivek Ghelani

Generative AI has dominated headlines as a transformative and disruptive technology. But where it might make a really big difference is in an area that's not being much talked about until now—strengthening supply chains.

Artificial Intelligence (AI) is nothing new. It's been used since the 1950s. The use of AI in business expanded rapidly in the 1970s as the power of computers became faster, and data storage became cheaper. What is new is Generative Artificial Intelligence (Gen AI), which represents a significant leap forward in the evolution of AI. All the current buzz and press were triggered by the broad public availability of powerful Gen AI tools in 2023. By using a natural language interface, Gen AI bought the power of AI to everyone.

The focus of this article is how companies are starting to use Gen AI in third-party risk management today and to look at future applications. A lot has already been written about the governance and ethical issues related to Gen AI. Our aim is to provide insight into Gen AI's practical application to address specific challenges companies have in managing third-party risk across the full spectrum of compliance and Environmental, Social, and Governance (ESG) topics.

Along the way, we will provide some background on the common uses of AI in supply chain risk management and the fundamental advancement that Gen AI made in AI. The research for this article included interviews and group discussions with senior supply chain, legal, and technology executives in Ethisphere and Digital Supply Chain Institute (DSCI) member companies. This includes Dr. Dave Ferrucci, considered to be one of the pioneers of Gen AI for his work in leading the IBM Watson Team, that developed groundbreaking natural language processing abilities making him a seminal figure in the evolution of AI.

In addition to presenting practical applications, the article also identifies critical success factors for using Gen AI in third-party risk management. Many of these success factors are applicable to any use of Gen AI.

AI AND GEN AI: WHAT'S THE DIFFERENCE?

Essentially, AI is a faster, more efficient way to process and analyze large amounts of data (structured or unstructured) to make decisions. There are several components under the AI umbrella, including natural language processing, optical recognition, and machine learning. AI follows defined rules established by programmers, and it can learn as it goes, which is the machine learning component. You may see this acronym used sometimes: AI/ML. The computer can get better at recognizing patterns and making predictions based on new data and previous examples. AI needs structured data and precise instructions (aka algorithms). The major challenges with AI are getting clean, structured data and ensuring that the algorithm is written to provide answers that address the business problem being solved.

Gen AI is the hot new, rapidly growing component of AI. It is a game-changer because it brings the power of AI to everyone. Gen AI opens up AI the way web browsers opened up the use of the Internet. It uses large-language models to search through structured and unstructured data to create something new. Gen AI can create new text, computer code, music, or images.

Gen AI responds to questions written in plain language, called prompts. The exact wording of the prompt has a significant impact on the answer that is provided. In fact, there's a new field emerging of "prompt engineers" that are trained to understand the business situation and translate it into an effective prompt. Gen AI systems are "trained" on data sets that can include public data and private data from your company. It's crucial to understand that the size and quality of these datasets play a significant role in determining the performance and biases of the AI model. At a simple level, the breakthroughs that make Gen AI so impactful are the ability of the computer to understand the context of each word and the ability to predict the next word in a sentence based on the context.

At a slightly more technical level, Gen AI has two game-changing elements:


CRAIG MOSS


VIVEK GHELANI

- Word embedding – words have meaning in their context and get meaning from the surrounding words. It's not just the context that gives meaning to these words but also their intrinsic semantic properties.
- Transformers – in developing the answer to the prompt, attention is paid to the context, and Gen AI predicts the next word(s) in the sequence. Transformers can capture complex relationships and dependencies between words in a sentence, enabling more coherent and contextually relevant outputs.

The major challenges with Gen AI arise from the lack of transparency in the computer's decision-making process because it uses deep learning and neural networks. As a result, the skill of the prompt writer is important, and there is no transparency related to the sources used to generate the answer. If the Gen AI has been trained on a data set that uses misinformation, the results will include misinformation. This lack of transparency has led to the need for an important new capability: data lineage. Data lineage is the ability to trace the source of data. More on the challenges and critical success factors for using Gen AI later in this article.

It may be helpful to think of AI as more quantitative and structured data processing and analysis, while Gen AI is more qualitative and creative with the ability to generate new, contextually rich content. Although Gen AI is in its infancy it is starting to change the way we work today and will definitely have a big impact on how we work in the future across virtually every function in an organization.

USE OF GEN AI IN SUPPLY CHAIN RISK MANAGEMENT

AI has established itself for years as a crucial tool in supply chain management. It enhances decision-making through predictive analytics, leading to increased efficiency in logistics, inventory management, and demand planning processes. AI's strength lies in its ability to process vast amounts of data, learn from it, and apply these learnings to improve performance over time.

Gen AI's unique ability to create and innovate is just starting to be used to improve the accuracy, efficiency, and effectiveness of compliance and ESG management programs. Let's look at some potential practical applications of Gen AI. No companies we interviewed are using Gen AI in the end-to-end ways we describe. We have taken the bits and pieces from early experiments and woven them together in practical applications for supply chain risk management.

Today, every company is on a tightrope trying to balance growing their business, ensuring supply chain resiliency, and addressing compliance and ESG risks and performance. The supply chain function is the bridge between internal silos and the suppliers that are critical to success. Based on research from the

MIKE CROWE ON THE CUTTING EDGE OF GENERATIVE AI

In the dynamic landscape of artificial intelligence, **Mike Crowe**, a retired Chief Information Officer, Co-Chair of the Digital Supply Chain Institute and an advisor to several tech companies, emerges as a thought leader. Here is a summary of our interview with him and his insights.

Mike emphasized the evolutionary nature of Generative AI. It is not a separate technology but a significant advancement within the broader spectrum of artificial intelligence technologies. Many business applications are going to involve multiple components of the AI suite, including Gen AI. He stressed that companies should start with the business problem they are trying to solve and define the desired outcome. Don't start by looking at this exciting new technology and trying to force its use into existing workflows.

Given his broad perspective, his views are particularly valuable on current uses. The most common use today is the auto-generation of tailored content, for example, images, marketing material, and email content. Mike does not see widespread use in supply chain risk management today, but he emphasized that companies are rapidly working to develop solutions that integrate Gen AI. He suspects that much of the practical application research being done today is by the supply chain software companies, including the supply chain risk management companies, seeking to incorporate Gen AI in order to advance their current offerings.

Mike anticipates the transformative power of Gen AI in supply chain risk management as part of a broader AI solution. He emphasized the importance of a robust data foundation and strategic implementation, cautioning against the rush to adopt Gen AI without proper data governance and quality controls. He advocates for beginning with small, manageable problems and gradually expanding, ensuring that each step is data-driven and aligned with specific business outcomes. This approach, he believes, is crucial for businesses to harness the full potential of AI and Gen AI without falling prey to the common pitfalls of overpromising how a new technology will revolutionize the business.

Mike's guidance serves as a vital resource for business leaders navigating the complex and rapidly advancing world of AI. His emphasis on foundational data infrastructure and controlled, purpose-driven application of Gen AI is particularly pertinent in today's technology landscape.

Digital Supply Chain Institute, forward-thinking companies are shifting their mindset from linear supply chains to multi-dimensional "constellations of value." The challenges in managing the risk have become even more pressing due to the rapid proliferation of supply chain due diligence laws.

Companies can have tens of thousands of third parties (e.g., suppliers, distributors, sales partners) spread across dozens of countries. The complexity is compounded because the risks vary dramatically depending on what the third party does and what jurisdictions apply. For example, a sales partner selling to government agencies may pose a very high corruption risk but a low environmental and labor compliance risk. Conversely, a manufacturing supplier may pose a high environmental and labor compliance risk but a low corruption risk. That's one area where Gen AI can help.

Gen AI can create tailored communications to third parties based on their jurisdiction and the most relevant risks. Communications that incorporate the provisions from your supplier code of conduct and the relevant laws can be created to set clear expectations for the third party. Gen AI can update the communications based on new regulations, updates to your supplier code of conduct or the changing focus of your stakeholders.

Think about the potential time-saving power of Gen AI in the full life cycle of managing third-party risk. Let's use data privacy as an example. You could use Gen AI to summarize the data privacy law of a certain country, then create a communication to all your third parties that operate in that country explaining your requirements for how they protect data. The communication could be tailored depending on the type of data they access or process and the related risk level. Then you could ask Gen AI to provide you with draft contracts that are aligned with the data privacy laws and your requirements. Going a step further, Gen AI could create simplified, plain-language (not legal language) data privacy policies to share with your employees by summarizing the relevant laws and contracts, then create training materials for your employees that interact with third parties. The training materials could include relevant data privacy scenarios based on their job function and a quiz. A short executive summary of your new data privacy program could be created for senior management and the Board. There's more. Gen AI could update the entire process and all the materials if the relevant law changes.

It sure sounds like a big time-saver. However, as we will discuss later in the key success factors section, expert human oversight and judgment remain essential.

Another emerging use for Gen AI as part of the overall AI system is in assessing and ranking third-party risk. Gen AI can compile and analyze structured and unstructured data from your internal sources, including company-specific and external public-sourced data. Imagine you have 100 manufacturing contractors in a country considered

high-risk for environmental and labor compliance. AI and Gen AI could be used to compile internal data sources like purchase orders, delivery schedules, labor compliance audits, and supplier performance reviews to identify any relevant patterns. For example, are there more labor violations when large orders are placed? Is there a correlation between on-time delivery and excessive working hours by factory workers? This internal data can be combined with a sweep of public data like news stories, participation by the company in industry-initiatives, and certifications they have achieved. Gen AI can help you synthesize the data on each of the 100 suppliers to create a company-specific risk profile and a consistent risk ranking.

"Gen AI does not give you the original sources it used, making it difficult to know if there are blind spots or biases in its sources."

Next is the ability for Gen AI to enhance existing AI systems to do pattern recognition and "what if" scenarios based on historical data and predictive analytics. You can simulate different scenarios and test the resilience of your supplier under various circumstances. This could help you assess the potential impact of disruptions or unexpected events. For example, what is the impact on labor compliance in the factory (e.g., excessive working hours) and on-time delivery if we make a change in the purchase order volume without changing the delivery date? What if we increase the order volume by 10%? What if we increase it by 30%? What if we change the materials specifications? What if we change the packaging material and design? A human expert would be critical to review the results and make the decisions, but Gen AI could rapidly develop several scenarios.

On a broader scale, Gen AI can generate a risk score and ranking for each supplier based on their specific activities for your company. This ranking can be used to prioritize your risk management efforts. It can offer tailored recommendations for mitigating risks with each supplier based on their activities, risk profile, and jurisdiction.

Gen AI could also provide insight on steps to take to improve your overall supply chain resiliency and highlight the potential trade-offs. This is very useful for gaining cross-functional support in your company between the legal, compliance, sustainability, and supply chain functions. For example, adding a backup component supplier close to your assembly plant may reduce geopolitical or weather-related business continuity risk, but it may increase the risk of losing your trade secrets and increase your cost per component because the order volumes are smaller. In this example, you can see the importance of wording the prompt to get a result that isn't biased to one functional area.

"Gen AI can generate a risk score and ranking for each supplier based on their specific activities for your company."

CHALLENGES OF GEN AI

Much has been written about some of the ethical and governance challenges of Gen AI. We are going to focus on the specific challenges of using Gen AI in supply chain risk management—although some of these challenges are also applicable to the use of Gen AI in other business areas.

The deep neural networks used by Gen AI are too complex to understand how it arrives at an answer. This is the core issue that has several practical implications. Compared to using an internet browser search, Gen AI does not give you the original sources it used, making it difficult to know if there are blind spots or biases in its sources.

The quality and accuracy of the Gen AI response are heavily dependent on the training data set and the prompt. Gen AI will mimic the data and documents it is trained on. This makes it important to understand to the extent possible what data was used in the training and generally what internal and external sources Gen AI accesses. Bias in the data training set or the prompt will influence the results. If there is misinformation in the data set, there can be misinformation in the answer. Going back to our examples, if a news article about a supplier incorrectly stated they had a data breach or serious labor violations, Gen AI would incorporate the false information into the risk ranking.

As mentioned earlier, this is leading to a relatively new field of *data lineage*—the process of tracking the flow of data over time, providing a clear understanding of where the data originated, how it has changed, and its ultimate destination within the data pipeline. Data lineage solutions seek to provide more transparency so people can trust the results because they trust the underlying data.

One of the challenges of using Gen AI is getting your people to trust the results, given a lack of knowledge about the data sources and possible lack of visibility into the prompt that was used if they weren't the ones writing the prompt. That's where data lineage comes in. A useful analogy is to think about data like water. We have probably all been in situations where we will readily drink from a glass of water because we trust the source of the water and its flow from the source to the glass. In other situations, we don't trust the water and refuse it, even if we are thirsty. More visibility into data sources and data quality builds more trust in the output, and trust in the output is critical to its usefulness.

CRITICAL SUCCESS FACTOR

First and foremost, know what problem you are trying to solve. Is Gen AI the right tool for the business problem you are trying to solve? Does it require the creation of new content? Is the output you are seeking language oriented? Does it require the synthesis and summary of several long documents? If it is, you must ask the right question. This is where prompt engineering comes in. Particularly if you are trying to solve problems that involve internal cross-functional teams, the prompt needs to be balanced in its approach. As we mentioned, one of the challenges of Gen AI is not knowing the sources that were used. This makes it even more critical to have transparency and consensus on the prompt. To build trust, record the prompts that are used and the corresponding Gen AI results. This tracking system will create more transparency in how Gen AI is used and can help educate users in better prompt writing.

Second, there must be sufficient controls in place to maintain data quality. This requires the orchestration of people, process, and technology. It involves some knowledge of the data set that is used in training the Gen AI system because the output is derived from the data it is trained on.

Third, it is essential to keep human experts in the decision-making loop today. Gen AI results must be monitored for "correctness." Is the answer within a reasonable range of answers? Just as with other compliance issues, you must establish your risk tolerance for "partially right" or "wrong" answers.

Fourth, leading companies are establishing cross-functional AI Committees to oversee the use of AI and Gen AI. These committees are charged with creating transparency, fairness, and governance policies and determining how to protect proprietary company information in Gen AI usage. For companies that are training their Gen AI using proprietary data sources and external sources, the protection of the proprietary data becomes another challenge and an issue that is critical to success.

WHERE TO START

Gen AI is here to stay, just like the Internet. It is a significant evolution in AI that dramatically lowers the barrier to using AI for businesses and subject matter experts. Now is the time to experiment and identify the best use cases for your company. For most companies the early applications of Gen AI are focused on creating targeted marketing communications, using Chat Bots for customer service, summarizing long documents, and computer programming.

Gen AI in supply chain risk management is at an earlier stage of development, but it will accelerate at an incredible speed. Third-party risk management is an enormously complex undertaking. Thousands of third parties. A wide range of compliance and ESG risks. Increasing regulations and reporting requirements. Huge amounts of data. More scrutiny from customers and investors. The confluence of these trends makes Gen AI a great solution.

In starting with Gen AI, don't make the mistake of starting with broad projects that are designed to completely replace existing workflows. Start with the problem and start small. Identify small specific problems in supply chain risk management where the output is language-based. Develop a plan for how you can link small projects into a more comprehensive end-to-end solution. Refer to the examples we provided in this article which are very narrow applications to an overall supply chain risk management program. Make sure to understand the data lineage and quality. Use your initial cases as a proof of value to make sure that there is a clear business benefit.

Ultimately, your job is to use human experts to carefully define the problem, ask the right questions, know where the data comes from, and make decisions based on the Gen AI outputs. ■

ABOUT THE AUTHORS

Craig Moss *is the Executive Vice President of Measurement at Ethisphere. He is also a Director of the Digital Supply Chain Institute. And he is Director-Content at the Cyber Readiness Institute and Chair of the Licensing Executives Society committee for developing an ANSI global standard for Intellectual Property Protection in the Supply Chain.*

Vivek Ghelani *is a Director of Research at Digital Supply Chain Institute, an applied research institute of the Center for Global Enterprise, a New York-based non-profit organization dedicated to studying contemporary corporations in the era of global economic integration. In addition to this role, Mr. Ghelani is a Senior Research Analyst at Mercator XXI, LLC., a professional services firm helping clients engage the global economy.*

CULTURE
corner
AN ETHISPHERE NEWSLETTER

DISCOVER CULTURE CORNER:

Your Ethical Culture Hub

Looking to enhance your ethical culture?
You've come to the right place.

Sign up today to get the latest best practices, training toolkits, and expert guidance. Learn how to cultivate a culture of integrity from the experts at Culture Corner.

SUBSCRIBE TO CULTURE CORNER NOW

Navigating Regulatory Tides

A Deep Dive into Fiscal Year-End SEC Enforcement Strategies

by Peter Chan, Karl Paulson Egbert, Jessica Nall, Jerome Tomas, Gavin Meyers, Matthew Smith, Jeffrey Butler, Kameron Hillstrom, and Katelyn VanDoorne

TADA IMAGES - STOCK.ADOBE.COM

The last thirty days in September, the end of the U.S. federal government's fiscal year, is generally an important time to analyze enforcement activity by the U.S. Securities and Exchange Commission (SEC). Because all enforcement cases must be reviewed and approved by SEC Commissioners, the end of the fiscal year often poses a logjam in processing enforcement recommendations. As a result, enforcement staff and leaders at the SEC must prioritize enforcement recommendations that they want to have approved by the Commissioners before the end of the fiscal year. Thus, in our experience, enforcement cases filed at the end of the fiscal year—particularly ones accompanied by a press release as opposed to a typical administrative or litigation release—are strong indicators of issues currently in the regulators' crosshairs and set the tone for enforcement hotspots and priorities for the next fiscal year.

Our key observations regarding the enforcement matters filed in this critical 30 day period in September with regards to overall SEC enforcement trends and policy messages include:

- A number of SEC cases reflect the enforcement message that self-reporting of misconduct by both public companies and financial firms as part of proactive cooperation will be rewarded, including potentially with settlements involving no civil penalties.
- The SEC will be aggressive in going after both companies and financial firms that include contract terms in employee agreements that are perceived to deter whistleblower complaints.
- The SEC is willing to pursue enforcement cases against financial firms and public companies based on strict liability violations that do not require intentional or even negligent misconduct.
- The SEC continues to scrutinize statements touting ESG capabilities and activities.
- A significant number of the SEC financial industry actions during fiscal year-end involve investment advisers, particularly those that are private fund managers, and allegations of violations of the marketing rules, custody rules, and breach of fiduciary duty relating

to conflicts of interest and overcharging of fees.

- The SEC continues to expand its enforcement of Regulation Best Interest against broker-dealers.
- Cases involving cryptocurrency and digital assets remain a priority.
- The SEC continues to focus on "off-channel" communications, reflecting a concern that broker-dealer and investment adviser supervision, as well as SEC investigations and examinations of financial institutions, can be circumvented by communications that are not maintained as part of required corporate books and records.

INCENTIVES TO SELF-REPORT: IT PAYS TO COOPERATE, OR AT LEAST COSTS LESS

The SEC has cooperation policies that encourage self-reporting of potential misconduct, but that fall short of proscribing detailed benefits to self-reporting entities as under the 2023 DOJ Voluntary Self-Disclosure Program. In the last 30 days in September, the SEC announced enforcement settlements that appear designed to highlight the potential financial benefits of self-reporting.

On September 7, 2023, the SEC announced settled charges against a financial services firm for failing to register the offers and sales of its retail crypto lending product. Despite the aggressive crackdown on the crypto industry, the SEC determined not to impose civil penalties due to the firm's cooperation and prompt remedial actions. In particular, following the SEC's February 2022 enforcement action against BlockFi, the firm voluntarily ceased offering its similar interest-bearing crypto lending product and returned all funds to its investors.

In a separate action involving a more traditional corporate accounting case, the SEC charged a public company with failing to disclose material information about unsupported adjustments the company made in several SEC filings, which increased the company's reported operating income by at least 15% in three quarters from 2019 through 2020. Again, the SEC determined not to impose civil penalties because the company promptly self-reported, undertook remedial measures and provided substantial cooperation to the Staff.

WHISTLEBLOWER PROTECTION: BOILERPLATE DISCLAIMERS IN EMPLOYEMENT AGREEMENTS MAY NOT BE SUFFICIENT

The SEC continues to aggressively enforce Rule 21F-17 under the Exchange Act against employment and other contracts with provisions that arguably chill whistleblower complaints to the SEC, regardless of whether the provisions were intended to deter such complaints. In the end of the fiscal year, the SEC highlighted its priority in this area by bringing cases against a privately held company and an investment adviser.

On September 8, 2023, the SEC announced it settled with a privately held energy and technology company for using employee separation agreements that violated the SEC's whistleblower protection rules by requiring certain departing employees to waive their rights to monetary whistleblower awards in connection with the filing of claims with or participating in investigations by government agencies. These provisions were determined to have raised clear impediments to participation in the SEC's whistleblower program. Jason J. Burt, Regional Director of the SEC's Denver Office, explained that "both private and public companies must understand that they cannot take actions or use separation agreements that in any way disincentive employees from communicating with SEC staff about potential violations of the federal securities laws," and "any attempt to stifle or discourage this type of communication undermines [the SEC's] regulatory oversight and will be dealt with appropriately." The company agreed to pay a civil penalty of USD 225,000.

On September 19, 2023, the SEC announced settled charges against a Dallas-based commercial real estate services and investment firm subsidiary of a publicly traded company for using an employee release that violated the SEC's whistleblower protection rule. According to the SEC's order, between 2011 and 2022, as a condition of receiving separation pay, the company required its employees to sign a release in which employees attested that they had not filed a complaint against the company with any federal agency. The SEC's order finds that by conditioning separation pay on employees' signing the release, the company took action to impede potential whistleblowers from reporting complaints to the Commission. Importantly, the SEC order found that a generic carve-out provision to allow for reporting to the SEC and other agencies was insufficient to remedy the impeding and chilling effect of the other provision. Noting the company's extensive remedial actions, the SEC imposed a civil penalty of USD 375,000.

On September 29, 2023, the SEC announced settled charges against a New York-based registered investment adviser for USD 10 million based on the adviser having raised impediments to whistleblowing by requiring employees to sign agreements prohibiting the disclosure of confidential corporate information to third parties (without an exception for potential SEC whistleblowers), and by requiring departing employees to sign releases affirming that they had not filed any complaints with any government agency in order for the employees to receive deferred compensation.

ESG: DO WHAT IS PROMISED

With the rise of Environmental, Social, and Governance (ESG) discourse, it is no surprise that the SEC is targeting companies that improperly promote ESG initiatives.

On September 25, 2023, the SEC announced charges against a registered investment adviser for

misstatements regarding its ESG investment process. To settle those charges and others, the investment adviser agreed to pay a total of USD 25 million in penalties. The SEC's order found that the investment adviser made materially misleading statements about its controls for incorporating ESG factors into research and investment recommendations for ESG-integrated products, including certain actively managed mutual funds and separately managed accounts. The order also found that the investment adviser marketed itself as a leader in ESG that adhered to specific policies for integrating ESG considerations into its investments. However, from August 2018 until late 2021, the investment adviser failed to adequately implement certain provisions of its global ESG integration policy as it had led clients and investors to believe it would. Additionally, the investment adviser failed to adopt and implement policies and procedures reasonably designed to ensure that its public statements about the ESG-integrated products were accurate.

We expect the SEC to continue its enforcement approach, including monitoring public statements by market participants and issuers regarding ESG topics. Given the lack of agreed upon definitions for each of the ESG categories, it will be important for both market participants and issuers to ensure that statements on ESG can be substantiated and that investors receive clear and full disclosure about how a statement on ESG was derived.

INVESTMENT ADVISER COMPLIANCE WITH CORE OBLIGATIONS WITH PARTICULAR FOCUS ON FUND MANAGERS

In a break from the typical spring-time announcement, the SEC released its 2024 SEC Exam Priorities on October 16, 2023 with the "hope that aligning the publication of our examination priorities with the beginning of the SEC's fiscal year will provide earlier insight to registrants, investors, and the marketplace of adjustments in our areas of focus year-to-year." Meanwhile, the SEC's fiscal year-end actions involving investment advisers, broker-dealers and clearing agencies reflected a focus on compliance with registrants' daily obligations.

Marketing Rule and Custody Rule Compliance: The SEC has been examining investment advisers for Marketing Rule compliance since the Rule went into effect last November and made clear a priority early on would be examining whether advisers adopted and implemented policies and procedures reasonably designed to achieve compliance with the Rule. On September 11, 2023, the SEC announced charges against nine investment advisers for violating the Rule by failing to do just that: focusing on the firms' failure to adopt and/or implement policies and procedures to address advertising hypothetical performance on their websites. In settling the charges, Gurbir S. Grewal, Director of the SEC's Division of Enforcement, made clear that the SEC would be continuing its Marketing Rule sweep efforts with a focus on the adequacy of policies and procedures, including hypothetical performance advertising.

On September 5, 2023, the SEC announced charges against, and settlements with, five investment advisers for failing to comply with core requirements under the Custody Rule, including performing audits, delivering audited financials to investors in a timely manner and ensuring a qualified custodian maintains client assets.

Undoubtedly, more enforcement actions related to the Marketing Rule will be forthcoming this fiscal year as the SEC's compliance sweep continues, and as noted its 2024 Exam Priorities regarding Marketing Rule compliance, the SEC staff will continue to make this an exam focus. While not a focus in the 2024 Exam Priorities, compliance with the Custody Rule is also a core investment adviser obligation and noncompliance can present significant risks. Moreover, the SEC proposed amendments to the Custody Rule early this year and is continuing to assess the proposal for enhancements.

Fiduciary Duty, Conflicts and Disclosure: Investment advisers should be aware that the SEC is focused on affiliate party conflicts of interest and is closely monitoring adviser duties to clients.

On September 5, 2023, the SEC announced an enforcement action against, and settlement with, a private equity firm focused on alternative real estate assets classes for failing to adequately disclose millions of dollars of real estate brokerage fees that were paid to a real estate brokerage firm owned by the CEO of the private equity firm. Osman Nawaz, Chief of the SEC's Enforcement Division's Complex Financial Instrument Unit, made clear that "information related to payments made to affiliates, and the potential conflicts of interest embedded in such arrangements, is critical to investors' decisions." The private equity firm agreed to pay the USD 20.5 million in penalties.

On September 12, 2023, the SEC announced a settled action against a company and its registered investment adviser subsidiary for failing to disclose critical information to investors in a USD 14.5 million asset-backed securities offering. Specifically, the company failed to disclose a heightened risk that it would be unable to seize assets in the event of a default and prior to the offering, the company had information showing that assets securing other loans that affiliates had made to the same borrowing group were reported as deconstructed without any notice or repayment or could not be located. Still, the company proceeded with the offering without disclosing this material information to investors.

On September 14, 2023, the SEC announced an enforcement action against, and settlement with, a Connecticut-based investment advisory firm and its owner for allocating profitable securities trades to favored accounts, including the firm's own accounts and client accounts that paid the firm a higher percentage of positive returns in fees. Andrew Dean, Co-Chief of the SEC Enforcement Division's Asset Management Unit, explained that "the SEC has the means to identify investment advisers that

abuse their position through cherry-picking, as [the firm and its owner] did." The firm and its owner agreed to pay USD 3 million in civil penalties.

On September 22, 2023, the SEC announced charges against, and settlement with, a California-based registered adviser to private funds resulting from acceleration of portfolio company monitoring fees, transferring a private fund asset from funds nearing the end of their term to a new fund and for loaning money from one private fund to another private fund advised by an affiliate.

Additionally, on September 26, 2023, the SEC announced settled charges against a New York-based advisory firm and its principal for failing to implement reasonably designed written policies and procedures concerning the disclosure of conflicts of interest. The advisory firm and its principal advised at least 13 clients to invest USD 6.1 million in three companies in which the principal had decision-making authority and significant ownership interests.

REGULATION BEST INTEREST CASES AGAINST BROKER-DEALERS

After bringing only a single enforcement action in all of 2023 involving Regulation Best Interest (Reg BI), the SEC squeezed in three new enforcement actions just under the fiscal year-end wire. Interestingly, the SEC chose not to announce these three cases in press releases, but in the more muted and less noticed form of administrative releases. It appears that the SEC wants to start treating Reg BI enforcement actions as routine, thus signaling additional cases are on the horizon. Therefore, we highlight these cases as they reflect the SEC's willingness to enforce less egregious Reg BI violations.

In line with its January 2023 Reg BI Risk Alert and 2023 Exam Priorities, each of the three actions dealt with one or more of the four core Reg BI obligations: Disclosure, Care, Conflict of Interest, and Compliance.

Disclosure Obligation: In one action, the SEC cited a broker-dealer for failing to make effective delivery of required Reg BI disclosures when attempting to deliver the disclosures electronically without meeting the SEC's requirements for electronic delivery: notice, access, and evidence of delivery (or informed consent). Of the three actions, it is notable that this one led to the largest fine. The action also is a reminder that the SEC has yet to adapt its electronic delivery guidance to the 21st Century.

Care and Compliance Obligations: In another action, the SEC charged a broker-dealer with violating the Care Obligation (as well as antifraud provisions of the federal securities laws) for excessive trading in customer accounts without regard for the associated transaction costs. The SEC also cited the firm for violating the Compliance Obligation by failing to establish, maintain and enforce policies and procedures reasonably designed to achieve compliance with the Care Obligation concerning excessive trading. The SEC also is litigating the same conduct in federal court against five of the firm's registered representatives. It is notable that the underlying conduct here could just have easily been brought under FINRA's prior suitability rule, and FINRA historically brought numerous cases involving similar facts under the prior suitability rule.

Conflict of Interest and Compliance Obligations: In a third action, the SEC focused entirely on the inadequacy of the broker-dealer's written policies and procedures with respect to Reg BI. Both the Conflict of Interest and Compliance Obligations explicitly require broker-dealers to establish, maintain and enforce written policies and procedures reasonably designed to achieve compliance with each of the Reg BI obligations, and, in particular, address conflicts of interest. While the firm had some written policies, they lacked guidance or actual procedures on how its associated persons could achieve compliance with the policies.

The string of actions are likely only a preview of SEC enforcement activity related to Reg BI that should be expected in the coming year. Coupled with Reg BI highlights in the 2024 SEC Exam Priorities, SEC enforcement will clearly be trending towards compliance with the substantive Reg BI obligations. As noted above, the SEC has yet to locate the distinguishable delta between the Care Obligation and the prior suitability rule in an enforcement action, but written policies and procedures will continue to be an area ripe for potential issues.

NO SLOWDOWN IN THE CRYPTO CRACKDOWN

The SEC has placed an emphasis on the crypto marketplace and participants, seeking to ensure that entities are regulated under existing marketplace structures and frameworks while still deliberating new rules and regulations. As we discussed elsewhere, on September 13, 2023, the SEC charged an entity with conducting an unregistered offering of crypto assets securities in the form of purported non-fungible tokens (NFTs) that raised approximately USD 8 million from investors to finance an animated web series.

We have frequently commented on the SEC's crypto crackdown since the fall of FTX late last year. Despite recent litigation losses, the SEC clearly will continue to test the bounds of its enforcement jurisdiction when it comes to crypto. As indicated recently by David Hirsch, Chief of the SEC's Crypto Asset and Cyber Unit, and reflected in the 2024 SEC Exam Priorities, the SEC will continue to be active when it comes to crypto investigations and enforcement.

PRACTICES INHIBITING SEC INVESTIGATIONS AND SURVEILLANCE REMAIN IN FOCUS

In contrast with lack of civil penalties for cooperating, the SEC imposed some of its stiffest penalties for practices that inhibit the SEC from conducting investigations and carrying out its market surveillance role.

Off-Channel Communications: On September 29, 2023, the SEC issued the latest actions in its ongoing crusade on recordkeeping violations related to off-channel communications, targeting broker-dealers and investment

advisers, as well as credit rating agencies. In some instances, the off-channel communications were discovered because firms could not produce communications to the SEC during investigations. The combined penalties from all of these actions exceeded USD 90 million across 12 firms. Notably, the SEC credited one firm in the recent sweep for self-reporting following an internal investigation initiated after firm staff identified business-related off-channel communications. The fine against that firm was millions less than the other firms included in the sweep, affirming the SEC's favorable view of self-reporting.

Registrants must establish strong protocols to ensure employees communicate via approved mediums in the first instance, and if the company finds there are off-channel communications, they must be preserved. With respect to broker-dealers and investment advisers, the SEC noted the off-channel communication violations were pervasive and longstanding, an indication that the SEC will be digging deep into firms' handling of unapproved communication channels.

Market Data Reporting Violations: In a similar vein to the off-channel violations, the SEC continues to monitor companies' other reporting requirements and in particular, blue sheet reporting. Blue sheet data is relied upon daily by the SEC and FINRA for market surveillance to detect insider trading and other market abuse practices. The SEC's latest action involving blue sheet data reporting compliance is a simple reminder of the importance that the SEC places on trade reporting generally. Given the various other trade reporting obligations of broker-dealers (CAT, OATs, TRACE, etc.), firms should be reviewing their reporting controls and processes periodically to ensure they are providing complete and accurate data. The firm received a USD 6 million civil penalty.

Incorrect Marking of Short and Long Sales: On September 22, 2023, the SEC announced settled charges against a broker-dealer for violating a provision of Regulation SHO, the regulatory framework designed to address abusive short selling practices, which requires broker-dealers to mark sale orders as long, short, or short exempt. These records are routinely used by regulators in policing prohibited short selling activity. To settle the SEC's charges, the broker-dealer agreed to pay a USD 7 million penalty.

According to the SEC's order, for a five-year period, it is estimated that the broker-dealer incorrectly marked millions of orders, inaccurately denoting that certain short sales were long sales and vice versa. The SEC's order finds that the inaccurate marks resulted from a coding error in the broker-dealer's automated trading system and that the firm provided the inaccurate data to regulators, including the SEC during this period. ■

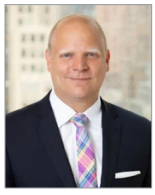
This article has been reprinted with permission and edited for length. To read the full version of this article, which includes additional insights on SEC Corporate Enforcement and Commodity Futures Trading Commission enforcement trends, please click here.

ABOUT THE AUTHORS

Peter Chan, *Partner, is a member of Baker McKenzie's North American Financial Regulation and Enforcement Practice.*

Jerome Tomas, *Partner, is co-chair of Baker McKenzie's North America Government Enforcement practice group.*

Jeffrey Butler *is an Associate in Baker McKenzie's Litigation and Government Enforcement Practice Group.*



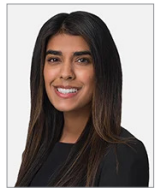
Karl Paulson Egbert, *Partner, is the co-chair of Baker McKenzie's Global Investment Funds steering committee and a member of the firm's Global Derivatives steering committee.*

Gavin Meyers *is a Counsel in Baker McKenzie's Transactional Practice Group in North America.*

Kameron Hillstrom *is an Associate in Baker McKenzie's Transactional Practice Group.*

Jessica Nall, *Partner, Jess leads Baker McKenzie's investigations and compliance practice on the West Coast.*

Matthew Smith *is a Counsel in Baker McKenzie's Transactional Practice Group and is a member of the Global Derivatives Team.*



Katelyn VanDoorne *is an Associate in Baker McKenzie's Litigation and Government Enforcement Practice Group.*

Baker McKenzie.

Calibrate Risk Globally

Whether dealing with high-stakes investigations, defending against government enforcement actions, or pursuing growth opportunities, success depends on calibrating risk.

With highly skilled lawyers on the ground around the world, we understand the regulatory, business and cultural landscape, wherever you are. And by connecting investigations and rapid crisis response with effective risk management solutions, our integrated approach helps you safeguard your business and protect corporate reputation.

Baker McKenzie—providing solutions for a connected world.

INVESTIGATIONS, COMPLIANCE & ETHICS

Climate, DE&I and Cybersecurity Disclosure Trends of the S&P 250

by Jennifer Cooney

The annual Labrador study of the S&P 250 companies' disclosure documents provide a valuable insight on what companies are sharing—and how they compare—when it comes to some of the biggest benchmarks in ESG.

Climate. Diversity, equity, and inclusion (DE&I). Cybersecurity. These three disclosure topics challenge even the most transparency-minded of U.S. reporting companies. Until recently, these topics were primarily addressed in annual environmental, social and governance (ESG) or sustainability reports and guided by reporting frameworks that were—key word to follow—voluntary.

Regulatory guidance, combined with investor and other stakeholder influence, pushed these three ESG topics into annual reports and proxy statements. What information is appropriate for which document confuses both individuals responsible for corporate disclosure and interested readers. Materiality, including the very definition of materiality and its application to each document, further complicates the puzzle.

As the Securities and Exchange Commission (SEC) begins to release final rules on these topics, there is a mix of trepidation (about potentially arduous requirements) and hope (for much needed clarity). When certain disclosures in annual reports on 10-K are required and other regulations are more settled, there is a sense that the level of detail and placement for supplemental information will fall into place. Information may still be spread across different reports, but a move toward standardization and appropriate cross-referencing should help provide a roadmap for readers and support information accessibility.

Labrador, an independent firm specializing in transparent investor and stakeholder communications, recently completed its annual study of the S&P 250 companies' disclosure documents, including proxy statements, 10-Ks, ESG reports, investor relations and codes of conduct. Evaluated against 237 discrete criteria that reflect the five pillars of transparency—accessibility, precision, comparability, availability and clarity—notable trends were uncovered in these documents relating to climate impact, DE&I, and cybersecurity disclosures that can help provide a comparative understanding of what other companies are sharing and where.

CLIMATE-RELATED DISCLOSURE

Climate reporting today for U.S. companies is driven primarily by stakeholder interest in ESG risks and opportunities. However, the SEC's climate disclosure proposal is looming, with adoption of new rules expected soon. Many of the S&P 250 also will be impacted by mandated disclosures resulting from the new California climate rules and the European Union's Corporate Sustainability Reporting Directive (CSRD).

This year's study found that there is a noticeable reference by the S&P 250 to ESG reporting frameworks and recommendations, including those of the International Sustainability Standards Board and its SASB Standards (90% of survey respondents), Task Force on Climate-Related Financial Disclosures (TCFD; 82%) and Global Reporting Initiative (GRI; 76%). Corporate familiarity with these frameworks is important. In particular, understanding the pillars of TCFD is critical because they form the foundational basis for many of the climate-related regulatory requirements to come.

Other key benchmarks to note:

- **Climate-Related Risks.** In 10-Ks, 80% of companies discuss environmental issues in the context of risk (compared to 65% in 2022). In ESG reports, 70% of companies explain how they identify, prioritize and manage climate risks and opportunities, and 40% share climate risk scenario analysis results.
- **Climate-Related Data and Goals.** In ESG reports, 92% disclose scope 1 and scope 2 emissions data year-over year (unless it is an inaugural report); 77% disclose scope 3 emissions data for the reporting year; and 90% report emissions reduction targets. In proxy statements, 53% note climate change/emissions goals.
- **Board Oversight.** In ESG reports, 71% of companies discuss the board's role in oversight of climate risks and opportunities. In proxy statements, 83% include a section, subsection or callout discussing the board's role in ESG (not climate-specific); 80% note distribution of ESG responsibilities to a specific board committee; and 35% state how often ESG is reported to the board.

DIVERSITY, EQUITY, & INCLUSION DISCLOSURE

With increased pressure from the SEC, investors and other stakeholders,

companies are releasing more workforce information. Providing accessibility to this information increases transparency and allows companies to be held accountable for their DE&I commitments. The SEC intends to propose new rules in the near future that would elicit more human capital management disclosure in 10-Ks, presumably with an emphasis on additional quantitative data.

It is clear from this year's study that DE&I is a priority for nearly all companies with disclosures warranting significant attention across all reports: 10-Ks (90% discussed DE&I in human capital management), proxies (86% addressed DE&I in human capital highlights) and ESG reports (95% included DE&I as a dedicated section, subsection or callout).

But there is still room for clearer, more illustrative information. For instance, in 10-Ks, only 58% of S&P 250 companies disclose global workforce statistics on gender, although this is an increase from 50% in 2022. Only 46% disclose workforce statistics on race, an increase from 39% in 2022. In ESG reports—where more granular data is typically included—clear presentations in graphic form showing the detail of diversity at various levels of the organization to enhance reader understanding could also use improvement.

Additional relevant findings:

- **Workforce DE&I Disclosures.** In ESG reports, 47% of companies present the gender diversity of the board of directors; 46% present gender diversity at the senior leadership level; 31% present gender diversity at the associate level; and 20% include all three in graphic form. Similarly, in ESG reports, 44% of companies present race/ethnicity diversity of the board of directors; 41% present race/ethnicity diversity of senior leadership; 29% present race/ethnicity of at the associate level; and 18% include all three in graphic form.
- **Board Diversity.** In proxy statement disclosures, 56% of companies include a dedicated section, subsection or callout explaining the company's approach to board diversity, including a policy or specific commitments; and 87% present board diversity information (individual or aggregated) in a matrix or table.
- **DE&I Goals.** In ESG reports, 49% of companies disclose DE&I goals and 45% of those companies also include progress against their goals.

CYBER SECURITY DISCLOSURE

The SEC adopted new rules in late July that will require companies to include annual disclosure requirements in their 10-Ks related to cybersecurity risk management, strategy, and governance, as well as file Form 8-Ks for material cybersecurity incidents.

The 2023 annual study revealed that 96% of S&P 250 companies currently discuss cybersecurity in the context of risk in their 10-Ks (at least at a high-level), and they are also beginning to address the related topics to varying degrees across their reporting documents in anticipation of the new rules. However, the risk management detail required by the new SEC rules—as well as the strategy and governance disclosures around cybersecurity - will require additional transparency and deeper context.

Current findings of note include:

- **Board Oversight.** In ESG reports, 52% of companies discuss the board's role in oversight of cybersecurity. In proxy statements, 57% include a dedicated section, subsection or callout discussing the board's role in oversight of cybersecurity (several companies also listed cybersecurity as an area of director continuing education)
- **Management Responsibility.** In ESG reports, 29% of companies state whether they have a Chief Information Security Officer or similarly titled position and to whom that person reports (54% say they have an officer, 30% disclose the reporting structure).
- **Risk Mitigation.** In ESG reports, 51% of companies disclose that they discuss monitoring and mitigation policies and practices; 54% present alignment with national or international standards like National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO); and 45% disclose cybersecurity training, including who is trained and how often (64% disclosed who is trained, 46% disclosed how often).

ADVICE FOR THE UPCOMING DISCLOSURE SEASON

While waiting for further regulatory instructions, companies should avoid slipping into a state of paralysis. Now is the time for internal and external reflection.

- Readiness assessments help to understand gaps between current disclosure practices and expected requirements.
- Companies should take a step back and make sure they can clearly articulate the connection between climate, cybersecurity and DE&I topics and their unique business strategy – as well as the supporting governance framework.
- At the same time, external engagement with investors and other known stakeholders can provide valuable insight into reporting expectations and readers' primary sources for company intelligence.
- The primary audience of each reporting document should be understood when considering voluntary topical disclosure.

ABOUT THE EXPERT

Jennifer Cooney *is the advisory practice director at Labrador U.S., a leading global communications firm focused exclusively on corporate disclosure documents. She has over 20 years of experience helping public companies report effectively to their shareholders and other key stakeholders.*

Managing Third-Party Due Diligence

When you're diligent about identifying risks, you'll have fewer of them

by Jon White

Third-party due diligence requires not only rigorous assessments, but continuous monitoring and foundational improvement to promote change within your program. The process for the past five years should be often revisited and revised to meet specific requirements.


JON WHITE

In discussing the many trial and error procedures that he embarked upon throughout his life, American inventor Thomas Edison once said, "I have not failed. I have just found 10,000 ways that won't work." Sometimes that is how it can feel for compliance professionals. We deal with risks associated with potential failure every day, but at the same time, we know we don't have the luxury of avoiding risk. Instead, we must mitigate it.

Risk levels are increasing, and third-party violations are a chief compliance concern for executives across industries. While strategic third-party relationships may expand opportunities, they also usher in significant risks both in terms of compliance and broader reputational exposure.

Due diligence is the process used to bring a business closer to its partners and it allows them to gain a deeper understanding of their unique risk profiles. It requires gathering sufficient

"At Omega Compliance, we apply a basic criterion across different markets where we are assessing third parties. For example, we review the costs of the contract—it could be a service or a product—and measure it against the value of that third-party relationship in terms of dollars and risk."

evidence to evaluate whether a partner is the right fit for you. In "Edisonian" terms, when you flip the switch when evaluating a potential partner, does the light bulb go on?

This process allows you to gauge if your partners will operate ethically and in compliance with applicable laws and any policies you may require them to follow. The due diligence process should be transparent and include the ability to continuously refine and improve, since keeping pace with risks are evolving faster than a company can manage. And yes, you may find ways [hopefully not 10,000] that won't work on your way to finding the ones that do. That is certainly my experience.

The truth is you cannot eliminate all risks, you can only contain them by implementing procedures and oversights that assuage those risks. Of course, we strive to eliminate potential issues that arise during the due diligence phase, but we must accept certain realities that limit our ability to guarantee 100 percent success, including the impact of varying government regulatory oversight (or the lack thereof) from country-to-country and geopolitical instability. We can chase perfection, but only if we are willing to accept excellence as a very strong consolation. Companies that understand this will have an advantage. Edison did. He chased excellence and founded General Electric. Not too shabby.

SCREENING: PARTNERING WITH BUSINESS TEAMS

At Ethisphere's recent 2023 South Asia Ethics Summit, I had the opportunity to lead a session on effectively managing the third-party due diligence process. This session included insights from John Deere and HCLTech. During that conversation, we took a closer look at how business teams are brought into the assessment of a third-party phase to assist in determining if the risk is acceptable or not. While every company has a slightly different approach—and this is dependent on their unique risk profile, tolerance, and locality—cross collaboration and leveraging the insights from business teams remain a critical factor in the overall third-party due diligence process.

CUSTOMIZING PROGRAMS FOR EACH MARKET

According to the panel, a rigid due diligence checklist is one way to effectively manage the third-party due diligence process. For example, at HCLTech, the checklists are very detailed, and encompass various components of the process, such as antibribery, anticorruption, pending litigation, and now, ESG execution and reporting. The scope of the due diligence checklist continues to evolve based on the unique risks and region-based regulations. Add to that the fact that our world has never changed at a faster pace than it does today. Therefore, the checklists are forever in flux, while the principles of risk management remain constant.

At Omega Compliance, we apply a basic criterion across different markets where we are assessing third parties. For example, we review the costs of the contract–it could be a service or a product—and measure it against the value of that third-party relationship in terms of dollars and risk. We consider all the factors—as risks can become complex. The location, stability, and overall reputation of that potential partner as well as other factors such as leadership and whether their culture is a match for our client. All these factors (and more) apply to a sound due diligence program when working with third parties.

Legendary Investor Warren Buffet, like Edison, is considered a pioneer in his industry and once said, "risk comes from not knowing what you are doing." It's a pretty simple comment from the world's longest serving, and arguably most successful CEO, but it's also very true. You can encapsulate the "why", as in "why we conduct due diligence," in that one phrase. All told, when you're diligent about identifying risks, you'll have fewer of them. ■

ABOUT THE EXPERT

Jon White *has held senior leadership positions, overseeing global supply chain compliance operations, for more than 20 years. He has extensive experience developing supply chain compliance and anti-corruption programs for many of the largest consumer brands and retailers in the world. Jon has been the Managing Director at Omega Compliance since its inception and continues to lead the company as its services grow. He can be reached at jwhite@omegacompliance.com*

Excellence in Action

Speak-Up Culture Best Practices from **WSP**, **Unum**, **Turner Construction**, and **SABIC**

by Bill Coffin

As part of Ethisphere's mission to help organizations around the world advance and evolve their ethics and compliance programs, we are in a unique position to showcase those companies whose programs truly exemplify the forefront of the E&C discipline.

By way of the rigorous Compliance Leader Verification process, Ethisphere can identify areas of strength and improvement around six key areas: program resources and structure; perceptions of ethical culture; written standards; training and communication; risk assessment, monitoring and auditing; and enforcement, discipline, and incentives.

This process doesn't just identify outstanding practitioners of ethics and compliance, but it also highlights those aspects of the discipline that carry special significance in today's ethics economy. One of those is the importance of speak-up culture. And as you read the insights from the four companies showcased in this feature, every one of those companies treats speak-up culture as a top priority that underpins an environment of ethics, accountability, and integrity.

WSP


MARIE CLAUDE DUMAS


JULIANNA FOX

*Based in Montreal, Quebec, **WSP** is one of the world's largest professional services firms providing strategic advisory, engineering, and design services to clients seeking sustainable solutions in the transportation infrastructure environment, building energy, water, and mining sectors. Earlier this year, Ethisphere granted Compliance Leader Verification to WSP for a second time in recognition of its exceptional ethics and compliance program. For **Marie Claude Dumas**, president and chief executive officer of WSP in Canada, and **Julianna Fox**, WSPs Chief Ethics and Compliance Officer, these recognitions are milestones in a never-ending pursuit of best practices that build a culture of ethics and integrity.*

Marie-Claude: I often compare ethics and compliance to health and safety in our industry. Those values are non-negotiable. We will never compromise on ethics and compliance. It's about having the ethics and compliance teams visible so that people know how to reach them. We want to make sure that we have a speak-up culture, but speaking up and making sure that employees feel safe and that there will be no retaliation, that's also very important. And it's also about being proactive.

Julianna: We run a global program, but there are regional and local realities and different of risks that at the regional and local level have to be addressed in a unique way. For instance, you talk about speak-up culture, which is something we've really been pushing for over the past few years. A healthy speak-up culture is not the same in the U.S. or Canada as it is in Asia or Latin America. So it's really about tailoring those KPIs and making sure that the program fits for each region.

We wouldn't be here without our stakeholder collaboration with units like

internal audit, HR, and communications as well as key stakeholders like our regional CEOs, our business line leaders. It is critical to get them to champion the program, not just from a tone at the top perspective, but to get people to want to meet KPIs because there's a reason behind why we are monitoring things, for example, like speak up ratios. That's how we've managed to gain traction with stakeholders: by partnering with them, talking to them, making sure it's on the agenda of executive level meetings and the global leadership team meetings in order to move forward together to implement that culture.

Marie-Claude: We first need to have that speak up culture. Then we also have metrics like compliance to training. Close to a hundred percent of our employees did the training, but we don't just do the training. We actually have ethics and compliance moments to discuss or case studies to discuss during management meetings or project meetings, real examples so that employees and leaders can relate in these gray situations. They're not theoretical examples. They're true.

Julianna: Ethics and compliance programs are usually centered on business integrity, integrity, respect, transparency, and we certainly embrace those here at WSP. In addition to our very strong focus on speaking up and on safety, feeling safe in the workplace and safety to speak up is a key value that we are embracing at WSP. And of course, the flip side of that is to have a very strong anti-retaliation policy in place.

Having Ethisphere come in is a lot of work, but it's completely worth it because you're able to assess the maturity of your program, identify areas of strength and areas of improvement, and really tailor your strategy based on that Ethisphere report. From my perspective, it's an exercise that's necessary to have an independent third party come in and make that assessment for you so that you can be clear sighted on which initiatives to focus on in the near future and long-term. For WSP—and I would assume for other organizations as well—these evaluations are a key part of our journey to continuously improve the program. ■

TURNER CONSTRUCTION

Turner

Turner Construction *is North America based, international construction services company and leading builder in diverse market segments. With a staff of over 11,000 employees. Turner has an annual revenue of $16 billion and complete some 1500 projects around the world, including schools and hospitals, stadiums and museums, airports, data centers, offices and more. But what sets Turner apart is its reputation for integrity, working safely, and its robust culture of ethics and compliance, as exemplified by the motto of its founder, Henry Turner: "A promise made is a promise delivered."* ***Ken Winfield****, Director of Compliance, lives that motto every day as he drives an ethics and compliance program where speaking up, safety, and success all go hand in hand.*

Our compliance program has provided us with a competitive advantage because clients understand our reputation for integrity and our ability to execute work in a in a transparent way. I really believe that that has been well received, not only internally, but externally as well. We have such a great organization and great employees, they really embrace the spirit of our core values, the idea of teamwork and working together holding each other accountable.

The idea of integrity is really sent from the top down. Our CEO does a weekly webcast, and one of the things he always talks about is the workplace being our home, and in our home, we do the right thing. If we see something wrong, whether that's a bias motive, an event, or a safety or a compliance issue, we speak up and call it out. We have the culture where we encourage our people to speak up, because workplace safety and strong ethical culture crossover quite a bit.

Workplace safety and a strong ethical culture are truly complimentary. Roughly five years ago, we launched our Active Caring Initiative, which started with safety. We used to walk on our construction sites and engage with our trade partners in a more punitive tone. "Why don't you wear your hardhat? Why aren't you wearing your glasses?" But now, if we are on a site and we see someone hammer drilling on a ladder, where they probably should have some sort of eye protection, for example, we'll ask, "What's wrong? Is


KEN WINFIELD

there an issue? Do you have a cheap pair of safety glasses? Here, take a better pair, they're not going to fog up, they're comfortable, you're going to want to wear them." Understanding what the issues are, we can take a practical, problem-solving approach.

We've taken this same approach to compliance, which is really an extension of Active Caring, where we are entrusting our people and empowering them with the responsibility to make good decisions. But we're also giving them the resources to ask questions and raise concerns. You have to have

a team approach. And it has to have the right tone from leadership. But you also have to support senior and middle management. It's important to explain the why to our people so they understand that the policies in place are guiding values, but they also protect both the individual and the company.

I think one of the key things that we have done as a company is doing a better job of explaining to our people the importance of compliance, as it relates to our day-to-day operations. It's not something extra that we're asking our people to do. They're already doing these things. They already treat our clients and our trade partners with integrity. They are already keeping accurate records and being transparent. If you have the support of your leadership and the support of the organization, then you just take it step by step. Establish a policy, focus on communication, make sure the guidelines are clear for people to follow. And really give them the means to raise concerns.

I really appreciate the work that Ethisphere does. We've been evaluated by Ethisphere for the past three years, and we use those recommendations to build and improve our program as part of our theme of continuous improvement.

SABIC

***SABIC** is one of the world's largest chemical manufacturing companies, with more than 31,000 employees in 50 different countries. Based in Riyadh, Saudi Arabia, SABIC's focus on ethics, compliance, diversity, culture, and anticorruption are just some of the program maturity hallmarks that have earned the company its Compliance Leader Verification status from Ethisphere. **Bo van Zeeland**, GM & Global Chief Counsel, Business Ethics & Compliance, notes that speak-up culture is an intrinsic part of SABIC larger integrity objectives, and that the challenge of creating a single speak-up culture across an organization with so many real-world cultures provides some unexpected opportunities for success.*

We invest heavily in an open and inclusive speak-up culture. We have various speak-up channels, whistleblower policies, and a network of more than 150 integrity ambassadors. But there's always room to improve. Like many other companies, we have hot spots. But we also have cold spots where reporting is too low. When we find those, we go out to them and have dialogues, identify root causes, and do something with that information to improve the speak-up rates. In the end, our employees are the eyes and ears of our program, and we need all of their help if we are to improve.

Speak-up culture does not just benefit integrity and compliance. It benefits our innovation culture. If people can speak up freely without fear of retaliation for reasonable failures and mistakes, then they will be in a zone of psychological safety that will make the company more able to learn from its mistakes, improve, be a better innovator, and be a stronger competitor in the market.

We regularly pulse the perceptions of employees about our program. Part of that is the willingness of people to report. If they're not willing to report, why not? This year, we are trying to integrate that into a survey that our HR department is conducting, which will help us to have integrated data. Which, of course, very helpful for us to advance.

In an industry such as ours, where there's a lot of performance KPIs, it's very important that we have managers and not the compliance team to talk about how we don't accept cutting corners on compliance. We want to make sure that people are reporting and that we're not misclassifying incidents, even when it comes to safety. We need people to bring forward what needs to be brought forward for us to identify and mitigate risks. I think a challenge a lot of companies face, SABIC included, is striking the balance between fairly disciplining misconduct when you find it, but not over-disciplining such that people become afraid to report. Some mistakes should be acceptable, and you should strike a balance so people come forward. You don't want to silence your own organization.

We are a culturally diverse organization, active in more than 50 countries. Process, procedure, and fairness should be consistent across regions and across countries. But we also have to recognize that there are different cultures, and pockets of cultures within the organization. What people have been taught when they were growing up, and how they have lived in and out of work can be very different from other parts of the organization. That is why we try to make people aware of our diversity and to embrace it. When people are aware of our differences of cultures and diversity, that makes us strong. But then we also are aware of our commonalities and the same drivers and goals that we all strive for.

UNUM

***Unum** is a leading provider of employee group disability, dental, life and critical illness insurance, based in Chattanooga, Tennessee. Unum has been honored as one of the World's Most Ethical Companies and recently earned Ethisphere's Compliance Leader Verification recognition for its outstanding program and practices. **Beth Simon**, Chief Compliance and Ethics Officer notes that the program draws on an organizational culture of ethics, robust relationships with other control functions like audit and risk, effective training and communications, and a strong tone at the top set by senior leadership. But through it all runs a speak-up tradition where the culture's own willingness to call out issues creates a virtuous cycle to everyone's benefit.*

We really try to build strong and trusted partnerships with our key stakeholders throughout the company. We try to understand their goals and initiatives and spend time listening to what's important to them. When we have that solid trust with our partners, and we do have a compliance or ethics challenge, the relationship is already there.

Something that has made us effective is the tone and the support that we get from our senior leaders. They understand how important ethics and compliance is to our company purpose, so they always raise their hands to help us out if we need a spokesperson. People expect people in compliance and ethics to talk about compliance and ethics, so it's wonderful we have leaders outside of our team talking about it. We have multiple leaders throughout this company who are more than willing to do that.

When you ask people, "Can you support us?", most will say yes, but they don't know what that looks like. So, we try to have a very specific ask, whether that's reminding teams to take compliance training on time or getting messages out during compliance and ethics week or asking them to have a discussion at their staff meeting about an ethical dilemma. And then we arm them with the right tools and communications to be successful. For example, we've developed a Leading with Integrity toolkit to make it easy for managers to have conversations with their team members around creating an environment where employees feel free to speak up.

We are very honored to have received these recognitions from Ethisphere. It's a real testament to the company's commitment to a compliant and ethical culture, how we serve our customers and our communities, and how we show up for each other every day. It is super important to our stakeholders, and I think it's a differentiator in the marketplace. When you have a company like Unum that can point to validation from external party like Ethisphere, it really does make a difference.

- Make sure that you have the right people on your staff. I am very fortunate to have a great team, so make sure you have the right people and the right skill set.
- I love going back to the basics and pointing to the Department of Justice guidance for corporate compliance programs as a guidepost for how you think about your program.
- Assess your company's compliance and ethics risk. It's going to look a little bit different for everybody, but that really helps you point your resources in the right direction.
- Build those partnerships. Really invest in that early and often.
- Communicate, communicate, communicate. You cannot talk enough about how important this is. I think people take for granted that doing the right thing comes naturally—and I think it does—but I think having that message out all the time, being delivered through various channels by different people, just makes it top of mind for employees, so they know how important it is to us as a company. ■


BETH SIMON

To learn more about Ethisphere's Compliance Leader Verification program, visit Ethisphere.com.

By the Numbers

THE YEAR OF GREAT EXPECTATIONS

2023 was a massive year for artificial intelligence (AI). Though the technology has been in development for decades, it wasn't until late 2022 when generative AI tools like ChatGPT arrived and created a frenzy of interest and activity in 2023. 2024 may prove to be the year of the great AI disappointment, however, if this technology's expectations outstrip its capabilities. But until then, this is AI's world. We're just living in it.

5

hours is all it took for ChatGPT to gain one million users after it launched in November 2022, making it the fastest-growing consumer app in history. It currently has over 180 million users... and climbing. Reuters

38.1%

Is the projected compound annual growth rate for the corporate adoption rate of AI between 2022 and 2030. At present, approximately 4 in 10 organizations plan to utilize AI. Grand View Research, Adobe

90%

of all customer interactions are expected to be AI-assisted by 2025. Only 7% of people trust chatbots, compared to the 49% that trust human advisors. AI Business, Gartner, Accenture

46%

of Product Development teams are projected to consider AI a critical capability of their function by 2025. Marketing and advertising (44%), HR (39%) and Sales (37%) are close behind. MIT

Technology: A game changer for compliance and ethics programs of the future

EY Forensic & Integrity Services can help transform compliance and ethics programs with technology solutions.

Get in touch to know more

EY
Building a better working world

More Human Than Human

by Bill Coffin

On Nov. 27, *Futurism* reporter Maggie Harrison broke a story that revealed how *Sports Illustrated* had not only been publishing AI-generated stories and not disclosing their origins, but they also used AI-generated author profiles for said pieces. Then, they deleted those avatars when questioned about it, in an apparent effort to conceal their use of AI. The story went viral and about a week later, two senior executives at *SI* publisher The Arena Group were let go as part of a restructuring. In a company call, Arena Group majority owner Manoj Bhargava told staffers: "Stop doing dumb stuff." Since then, the Arena Group has fired Sports Illustrated CEO Ross Levinsohn, who has been replaced in the interim by Bhargava. You can read all about it here, here, here, and here.

One can imagine why somebody like myself might get so out of joint over the rise of tools like Midjourney and ChaptGPT, which have both caused such a stir this year. And I get it. Johannes Gutenberg put an awful lot of scribes out of business. And this issue's digital publication represents no small amount of money that hasn't gone to a commercial printer. The tides of technology reshape business all the time, and part of our modern professional skillset must be the capacity for evolution.

That said, there is something deeply disquieting about the current state of AI as a tool for generating media content, and the *SI* debacle underscores it perfectly. When a media company switches over to using AI as a means of creating content, it sets the psychological safety meter of the organization to zero, because it tells the core of its workforce that management would rather not pay for them. Going forward, that's a big self-inflicted wound for an organization to address if they intend to retain the people who haven't yet been replaced by machines.

The ethical considerations here are even more profound. We all know businesses require a social license to operate. For media brands, that license depends on transparency and accountability. When a publisher tries to create a new content model based on a complete lack of transparency, and they do so surreptitiously with an intent to obscure and deceive—then they have shattered the trust placed in them by their audience.

I would like to think that this is merely a one-off case of a rogue publisher. But I personally know professional writers and artists whose work has been scraped without consent or compensation by large technology companies to train their AI models. When an entire technology appears to have been developed and rolled out with a certain degree of bad faith built into it, at some point, we should question the technology, those behind it, and those most eager to use it.

It is so easy to use AI and not admit it. And therein lies a potential contagion of dishonesty that threatens to infect the whole of business content and communication, fostered by the naïve and the nefarious alike. And if that sounds like a Luddite alarm, let me leave you with this:

Ethisphere Magazine was approached for this very issue—the theme of which is Ethical AI—by a company that wanted to submit a story for publication about how companies can develop an AI strategy. The story displayed numerous red flags that it had been written in whole or in part by AI. When the submitter was asked about it, the submitter raised similar red flags that they, too either were generated by AI themselves, or they used AI extensively to communicate. When asked to prove they were not an AI by appearing on camera in a call, they ceased communication. If you had asked me when I graduated from college if, one day, I would be conducting Voight-Kampff tests on magazine authors, I would have told you to watch less *Blade Runner*. And yet, here we are. So, if you'd like to publish in *Ethisphere Magazine*, we would love to have you. Just so long as first, you tell us in single words, only the good things that come into your mind about your mother. ■

BILL COFFIN
Editor in Chief

ETHISPHERE

ETHiCAST

Your New Favorite Ethics & Compliance Podcast

Subscribe Today

NEW EPISODES WEEKLY

music

★ SUPPORT NEEDED ★

I wish to have a backyard makeover

Kylie, 12
cancer

DON'T WAIT FOR HOPE. *Create it.*

Hope is essential for children with critical illnesses, and you can unlock its life-changing power today. Help make wishes come true.

DONATE TODAY AT WISH.ORG

Make-A-Wish®