COSMOS
Navigate the Compliance Universe

CEP Magazine - October 2022

Lee Tiedrich (lee.tiedrich@duke.edu) is the Distinguished Faculty Fellow in Ethical Technology at the Duke Initiative for Science & Society, has a dual appointment at Duke University Law School, and is a member of the Global Partnership on AI (GPAI) Multistakeholder Expert Group. Before joining Duke, she was a partner at an AMLaw 100 law firm, co-led the global and multidisciplinary Artificial Intelligence Initiative, and held other positions.

Data and emerging technology: The new ethics and compliance frontier

By Lee Tiedrich

Companies are investing significantly in digital transformation, data, artificial intelligence (AI), and other emerging technologies (collectively, digital tools). PwC reports that 60% of surveyed executives identified digital transformation as "their most critical growth driver in 2022."[1] International Data Corporation (IDC) projects that digital transformation spending will "reach $2.8 trillion in 2025, more than double the amount allocated in 2020."[2] Not surprisingly, emerging technologies have experienced similar growth. AI reportedly had a market value of $93.5 billion in 2021, and this market value "is projected to expand at a compound annual growth rate … of 38.1% from 2022 to 2030."[3] Similarly, the metaverse market could reach $800 billion by 2024.[4]

This trend extends across many industries, including manufacturing, healthcare, financial services, defense, automotive, consumer products, and others not traditionally associated with technology. For instance, McDonald's has invested in AI to enhance its customer experience,[5] and Domino's has become a "truly digital–first business."[6] IKEA employs AI and augmented and virtual reality to help consumers visualize furnishings in their homes,[7] and chatbots have become staples in customer service. Data and AI are also increasingly used to support human resource functions, supply chain management, and other internal operations.

As companies strive to harness the benefits of digital tools, compliance departments should adapt to support them. To begin, compliance departments should familiarize themselves with the relevant digital tools and their potential benefits and risks. Additionally, compliance departments should implement strategies for managing the risks in ways that also help organizations capitalize, in a compliant and trusted manner, on the beneficial uses of digital tools.

Understanding risks

The precise risks associated with a digital tool may depend upon various factors, such as its intended and potential unintended uses and design. Therefore, compliance departments need to understand the relevant digital tools, including their operation and possible uses. To illustrate, "harmful discrimination" is a potential risk associated with AI. Compliance departments are better positioned to address this risk if they understand how "training data" and other factors can lead to discrimination and how "black box" algorithms can create a lack of transparency. This section describes some broad categories of risks that can arise with digital tools and how they can impact organizations.

Reputational harm and liability

Even if unintended, improper use or processing of digital tools can result in reputational harm and increased liability risk. For instance, Amazon experienced backlash and stopped deploying its AI recruiting tool because it inadvertently discriminated against women.[8] The U.S. Equal Employment Opportunity Commission (EEOC) and the U.S. Department of Justice (DOJ) have warned that AI tools can violate antidiscrimination laws. The EEOC has issued guidance for avoiding such unlawful conduct,[9] and it recently brought a complaint against a company that allegedly used a digital tool to unlawfully discriminate against job applicants based on age.[10]

This increased government scrutiny is not limited to the employment context. For example, the Federal Trade Commission (FTC) recently issued an advance notice of proposed rulemaking on commercial surveillance and data security.[11] In addition, the FTC recently required the disgorgement of two AI algorithms trained on data without proper consent and has published AI guidance.[12][13][14] Relatedly, the FTC has warned organizations that collect sensitive consumer data that it is "committed to using the full scope of its legal authorities to protect consumers' privacy."[15]

In addition to collaborating with the EEOC, DOJ has launched an initiative to combat redlining.[16] It also recently settled antidiscrimination cases against Trustmark National Bank (also involving the Consumer Financial Protection Bureau (CFPB) and Office of the Comptroller of the Currency (OCC))[17] and Meta relating to digital tools used in connection with lending and online housing advertisements, respectively.[18]

The risk of reputational harm and liability extends beyond discrimination, data privacy, cybersecurity, and government enforcement. For example, an Uber self-driving car inadvertently killed a pedestrian because it could not recognize jaywalkers.[19] Reports of groping and other harassing conduct on Meta's virtual reality platform have surfaced.[20] And at least some emerging technologies could become new frontiers for litigation.[21]

The evolving landscape

The legal, policy, and standards landscape for digital tools is changing rapidly, which increases the risk of noncompliance for organizations and presents business challenges. In addition to the increasing government enforcement discussed above, there is a significant uptick in newly adopted and proposed laws and regulations applicable to digital tools. For instance, several American states have enacted privacy legislation. New York City has established auditing requirements for AI hiring tools,[22] and Colorado has prohibited insurers from using external consumer data and algorithms to discriminate unfairly. On the federal level, Congress continues to consider enacting privacy and AI legislation, such as the American Data Privacy and Protection Act and the Algorithmic Accountability Act, respectively. And federal agencies, such as the U.S. Food and Drug Administration and the U.S. Department of Defense (DoD), are also addressing digital tools.

Significant developments also are occurring within standards bodies and internationally, such as in the European Union (EU), where the proposed Artificial Intelligence Act (EU AI Act) would regulate AI offered within the EU. Companies need to be aware of this proposal now, so they can start factoring it into product designs and plans. For example, the proposed EU AI Act would ban certain AI uses and regulate others, such as a broad category of "high-risk AI" that would be subject to a wide range of premarket and postmarket requirements. Violators could face hefty penalties. Given the draft EU AI Act's significance, setting the groundwork now to adapt to it can reduce business uncertainties.

Employee, investor, and board scrutiny

Employees, investors, and corporate boards also have sharpened their focus on digital tools. For example, Google faced criticism from ethical AI co-lead Timnit Gerbu about discriminatory AI, culminating in her departure.[23] It also recently dismissed an engineer following his claim that certain Google AI is sentient.[24] In 2018, Google did not renew its DoD contract for Project Maven after employees expressed concerns about using technology for advanced weaponry.[25] Last year, Facebook whistleblower Frances Haugen came forward alleging, among other things, that Facebook knew its products were harming teen mental health.[26] Haugen also filed SEC complaints asserting that Facebook did not accurately disclose its misinformation practices to investors.[27]

Relatedly, investors increasingly are evaluating AI governance, and more organizations recognize that AI ethics is part of environmental, social, and governance (ESG) activities and corporate social responsibility. Corporate boards are seeking to increase their expertise and oversight of digital tools.