

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 Gebru 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.

Proactively addressing risks

Compliance departments can help address the digital tool risks in ways that also assist organizations in unlocking their benefits. This section describes some strategies for achieving this goal.

“Ethics and compliance by design”

“Ethics and compliance by design” has emerged as a cornerstone for developing and deploying trusted digital tools. The goal is to embed ethics and legal compliance as well as sustainability throughout the digital tool lifecycle and foster effective cross-disciplinary collaboration and the integration of diverse viewpoints. “Ethics and compliance by design” typically starts with the organization’s leadership adopting guiding principles (such as, in the case of AI, principles consistent with the Organisation for Economic Co-operation and Development AI principles and creating a governance framework. This governance framework should enable the organization’s compliance, legal, sustainability, and ethics specialists to provide regular input to the technology, data science, and business leads about legal and other factors that should be addressed in product design and later in the lifecycle. It also enables the business, data science, and technical teams to obtain timely inputs from compliance and other experts as questions or concerns arise during their work.

A holistic “ethics and compliance by design” program draws upon many core functions of compliance departments. For example, the program should include protocols for:

- Documenting processes and procedures
- Making and documenting decisions (and escalating them, as appropriate)
- Providing for training and proper notices
- Obtaining and managing consents
- Providing for accountability and an appropriate level of human oversight
- Keeping pace with the evolving legal, standards, and policy environment

It also should have mechanisms for appropriately responding to complaints, incidents, and concerns as they may arise.

In addition to reducing risk and business uncertainties and enhancing compliance and accountability, this approach positions organizations to provide better transparency and explanations to their many stakeholders.

Digital tool inventory

In connection with “ethics and compliance by design,” organizations should undertake and regularly update an inventory of existing and planned digital tools, including those used internally and externally. This exercise will further ensure that compliance efforts align with business objectives. It also will help pinpoint which of the myriad of legal, policy, and standards developments are most relevant to the organization.

Risk management

A consensus is emerging that effective governance also should manage risks. At the governmental level, for example, the draft EU AI Act would require “high-risk AI” to have a risk-management system, and the National Institute of Standards and Technology (NIST) has developed a draft AI Risk Management Framework (the AI RMF).

As part of risk-management efforts, organizations can conduct impact evaluations and assessments. These tools can help organizations proactively identify and understand the digital tools’ intended and unintended consequences and mitigate them as needed. Impact assessments are commonplace in privacy and other contexts and are gaining momentum for AI. For instance, the proposed Data Privacy and Protection Act would require AI design evaluations and, in some cases, AI impact assessments. The Algorithmic Accountability Act and the United Nations Educational, Scientific and Cultural Organization (UNESCO) Agreement on Ethical AI (UNESCO AI Agreement) include AI impact assessment requirements as well. AI impact assessments also have gained traction within industry as reflected by Microsoft’s recently published “Responsible AI Impact Assessment.”^[28]

Emerging policies focusing on risk management also underscore the need for ongoing testing and monitoring of digital tools and appropriate remediation procedures and human oversight, particularly when digital tools potentially can have material adverse impacts. Compliance departments are well positioned to help organizations implement these programs effectively.

Vendor diligence

Organizations often use digital tools developed by third-party vendors. As part of “ethics and compliance by design,” organizations should conduct due diligence on third-party vendors and tools before entering into contracts. The EEOC has provided some due diligence guidance for human resources digital tools.^[29] Unlawful discrimination can occur even when unintended. Furthermore, the DOJ and EEOC have clarified that legal violations can arise when employers use discriminatory third-party tools.^[30] The NIST AI RMF also highlights broadly the importance of supply-chain management.^[31]

Data governance

In addition to addressing data privacy and cybersecurity, organizations should establish a data governance program. This will help organizations understand the provenance and lineage of their data, which in turn should better enable them to (1) detect and address potential biases; (2) implement a consent and rights management system; (3) provide for better transparency, traceability, explanations, accountability, and data stewardship; and (4) help ensure that the data is suitable for its intended purposes.

Data governance is critical to compliance, particularly given the increasing government attention. Indeed, the

FTC has cautioned:

If a dataset is missing information from particular populations, using that data to build an AI model may yield unfair or inequitable results to legally protected groups. Think about ways to improve your dataset, design your model to account for data gaps, and—consider any shortcomings—limit where or how you use the model.^[32]

Other policymakers recognize the importance of data governance too. The proposed EU AI Act would impose data governance requirements on “high-risk AI,” and the UNESCO AI Agreement calls upon governments to “develop data governance strategies that ensure the continual evaluation of the quality of training data for AI systems.”^[33]

Crafting use cases and statements

Compliance departments also can help craft digital tool use cases that reduce potential risk and liability. As noted above, the FTC has emphasized the importance of addressing shortcomings in AI training data when specifying use cases. Explanations and public-facing statements for digital tools also should align with the relevant facts and laws to reduce the likelihood of engaging in unfair or deceptive trade practices or other unlawful activities.

There is at least one judicial case, *Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Sols.*,^[34] that reinforces the importance of carefully crafting digital tool use cases and public statements. In this case, the court held that an AI vendor could be liable for violating the Fair Housing Act’s antidiscrimination provisions and other laws when a customer relied on the vendor’s tool to unlawfully deny housing to a prospective tenant. In reaching this decision, the court noted that the AI vendor “had the power to end its discriminatory practice by modifying or discontinuing its . . . [screening tool] and offering only its . . . [other] product, but it refused to do so.”^[35] It also commented that the AI tool was “advertised as ‘automat[ing] the evaluation of criminal records, reliving your staff from the burden of interpreting criminal search results.’”^[36]

Conclusion

As organizations continue to invest in promising digital tools, compliance departments should prepare to assist them in achieving the desired benefits while addressing the potential harms and risks. To do this, compliance departments can draw upon their core strengths and functions. They must educate themselves about relevant digital tools and the evolving legal and policy landscape and help implement “ethics and compliance by design” governance programs tailored for their organizations that include the abovementioned steps.

The author would like to thank Kristi Boyd and Annmarie Messing for their assistance with this article, which is provided for informational purposes and does not constitute legal advice.

Takeaways

- Compliance departments should support companies in sustainably unlocking the benefits of digital tools in ways that address the increasing government scrutiny and mitigate risks.
- This requires using core strengths and implementing “ethics and compliance by design” governance frameworks that bring together diverse expertise and viewpoints throughout the lifecycle.
- These frameworks include documentation, decision-making, oversight, training, incident response,

accountability, and other mechanisms and enable organizations to adapt nimbly to an evolving legal environment.

- They also encompass other steps, including maintaining digital tool inventories and implementing risk management, supply chain management (including vendor due diligence), and data governance.
- Compliance departments should help craft digital tool use cases, explanations, and public-facing statements to help ensure they align with relevant facts and laws.

1 PwC, “PwC Pulse Survey: Executive Views on Business in 2022,” January 27, 2022, <https://www.pwc.com/us/en/library/pulse-survey/executive-views-2022.html>.

2 International Data Corporation, “New IDC Spending Guide Shows Continued Growth for Digital Transformation as Organizations Focus on Strategic Priorities,” news release, November 9, 2021, <https://www.idc.com/getdoc.jsp?containerId=prUS48372321>.

3 Grand View Research, “Artificial Intelligence Market Size, Share & Trends Analysis Report By Solution, By Technology (Deep Learning, Machine Learning, Natural Language Processing, Machine Vision), By End Use, By Region, And Segment Forecasts, 2022–2030,” report ID: GVR-1-68038-955-5, April 2022, <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market>.

4 Matthew Kanterman and Nathan Naidu, “Metaverse May Be \$800 Billion Market, Next Tech Platform,” *Bloomberg Intelligence* (blog), December 1, 2021, <https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform>.

5 Ryan Owen, “Artificial Intelligence at McDonald’s—Two Current Use Cases,” *Emerj Artificial Intelligence Research*, last updated January 26, 2022, <https://emerj.com/ai-sector-overviews/artificial-intelligence-at-mcdonalds/>.

6 Lucy Tesseris, “Domino’s to Invest £20m in Digital Acceleration,” *Marketing Week*, March 8, 2022, <https://www.marketingweek.com/dominos-invest-20m-digital-acceleration>.

7 Ingrid Lunden, “Ikea Acquires AI Imaging Startup Geomagical Labs to Supercharge Room Visualisations,” *TechCrunch*, April 2, 2020, <https://techcrunch.com/2020/04/02/ikea-acquires-ai-imaging-startup-geomagical-labs-to-supercharge-room-visualisations/?guccounter=1>.

8 Jeffery Dastin, “Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women,” *Reuters*, October 10, 2018, <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>.

9 U.S. Department of Justice, “Justice Department and EEOC Warn Against Disability Discrimination,” news release, May 12, 2022, <https://www.justice.gov/opa/pr/justice-department-and-eeoc-warn-against-disability-discrimination>.

10 U.S. Equal Employment Opportunity Commission v. iTutorGroup, Inc., No. 1:22-cv-02565 (E.D. N.Y. May 5, 2022).

11 Federal Trade Commission, “Commercial Surveillance and Data Security Rulemaking,” news release, August 11, 2022, <https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking>.

12 Federal Trade Commission, “California Company Settles FTC Allegations It Deceived Consumers About Use of Facial Recognition in Photo Storage App,” news release, January 11, 2021, <https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo>.

13 Federal Trade Commission, “FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids’ Sensitive Health Data,” news release, March 4, 2022, <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive>.

- 14** Elisa Jillson, “Aiming for Truth, Fairness, and Equity in Your Company's Use of AI,” *Business Blog*, Federal Trade Commission, April 19, 2021, <https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>.
- 15** Kristin Cohen, “Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data,” *Business Blog*, Federal Trade Commission, July 11, 2022, <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use>.
- 16** U.S. Department of Justice, “Justice Department Announces New Initiative to Combat Redlining,” news release, October 22, 2021, <https://www.justice.gov/opa/pr/justice-department-announces-new-initiative-combat-redlining>.
- 17** Consumer Financial Protection Bureau, “CFPB, DOJ and OCC Take Action Against Trustmark National Bank for Deliberate Discrimination Against Black and Hispanic Families,” news release, October 22, 2021, <https://www.consumerfinance.gov/about-us/newsroom/cfpb-doj-and-occ-take-action-against-trustmark-national-bank-for-deliberate-discrimination-against-black-and-hispanic-families/>.
- 18** U.S. Department of Justice, U.S. Attorney’s Office for the Southern District of New York, “United States Attorney Resolves Groundbreaking Suit Against Meta Platforms, Inc., Formerly Known As Facebook, To Address Discriminatory Advertising For Housing,” news release, June 21, 2022, <https://www.justice.gov/usao-sdny/pr/united-states-attorney-resolves-groundbreaking-suit-against-meta-platforms-inc-formerly>.
- 19** Phil McCausland, “Self-driving Uber Car That Hit and Killed Woman Did Not Recognize That Pedestrians Jaywalk,” *NBCNews.com*, November 9, 2019, <https://www.nbcnews.com/tech/tech-news/self-driving-uber-car-hit-killed-woman-did-not-recognize-n1079281>.
- 20** Tanya Basu, “The Metaverse Has a Groping Problem Already,” *MIT Technology Review*, December 16, 2021, <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/amp>.
- 21** Christine Schiffner, “As the Metaverse Expands, Lawsuits Could Soon Follow,” *National Law Journal*, June 6, 2022, <https://www.law.com/nationallawjournal/2022/06/06/plaintiffs-firms-eye-metaverse-as-growth-target-for-litigation/?slreturn=20220603182458>.
- 22** New York City Council, “Automated Employment Decision Tools,” law no. 2021/144, (2021), <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9>.
- 23** Karen Hao, “We Read the Paper That Forced Timnit Gebru Out of Google. Here’s What it Says,” *MIT Technology Review*, December 4, 2020, <https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru>.
- 24** Reuters, “Google has fired a software engineer who claimed an AI chatbot was sentient,” *NBC News*, July 23, 2022, <https://www.nbcnews.com/news/us-news/google-fired-software-engineer-claimed-ai-chatbot-was-sentient-rcna39679>.
- 25** Daisuke Wakabayashi and Scott Shane, “Google Will Not Renew Pentagon Contract That Upset Employees,” *The New York Times*, June 1, 2018, <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html>.
- 26** Dan Milmo, “Frances Haugen: ‘I Never Wanted to be a Whistleblower. But Lives Were in Danger,’” *The Guardian*, October 23, 2021, <https://www.theguardian.com/technology/2021/oct/24/frances-haugen-i-never-wanted-to-be-a-whistleblower-but-lives-were-in-danger>.
- 27** Ana Popovich, “Facebook Whistleblower Frances Haugen Files More Complaints with SEC,” *Whistleblower Network News*, February 19, 2022, <https://whistleblowersblog.org/corporate-whistleblowers/sec-whistleblowers/facebook-whistleblower-frances-haugen-files-more-complaints-with-sec>.
- 28** Microsoft, “Microsoft Responsible AI Impact Assessment Template,” June 2022, <https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-RAI-Impact-Assessment-Template.pdf>.
-

29 U.S Equal Employment Opportunity Commission, “The Americans With Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees,” EEOC-NVTA-2022-2, May 12, 2022, <https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence>.

30 U.S Equal Employment Opportunity Commission, “Artificial Intelligence to Assess Job Applicants and Employees,” questions 3 and 7.

31 National Institute of Standards and Technology, “AI Risk Management Framework: Initial Draft,” March 17, 2022, 19, <https://www.nist.gov/document/ai-risk-management-framework-initial-draft>.

32 Jillson, “Aiming for Truth.”

33 United Nations Educational, Scientific and Cultural Organization, “ANNEX VII Recommendation on the Ethics of Artificial Intelligence,” *Records of the General Conference: Volume 1, Resolutions*, November 2021, 159, <https://unesdoc.unesco.org/ark:/48223/pf0000380399/PDF/380399eng.pdf.multi.page=143>.

34 Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Sols., LLC, 369 F.Supp.3d 362, 366–381 (D. Conn. 2019), <https://www.ctfairhousing.com/PDFs/CoreLogicMTDOrder.pdf>.

35 Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Sols., LLC, 17–18.

36 Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Sols., LLC, 23.

This publication is only available to members. To view all documents, please log in or become a member.

[Become a Member Login](#)