Regulatory, litigation and disclosure considerations concerning artificial intelligence

DLA PIPER

Question:

What is the future of AI regulation?

ChatGPT:

It is difficult to predict the future of AI regulation with certainty, as it will likely depend on a number of factors, including advances in AI technology and how it is used, as well as changes in public attitudes towards the use of AI. However, it is likely that as AI technology continues to advance and become more widespread, there will be an increased need for regulation to ensure that it is used safely and ethically. This may involve establishing guidelines for the development and use of AI, as well as creating oversight mechanisms to enforce those guidelines. Ultimately, the goal of AI regulation would be to ensure that the technology is used in a way that benefits society, while minimizing any potential negative impacts.

Introduction

Note to readers: This article was not generated by ChatGPT. However, the attention surrounding the newest chatbot is representative of the growth in the use and influence of artificial intelligence (AI) and its potential implications across industries and society.

Global investment in AI is accelerating rapidly. According to the IBM AI Adoption Report (2022), **68%** of US companies have knowingly employed or are exploring adopting AI. Far more are using AI algorithms without knowing it. Private investment more than **doubled** from 2020 to 2021 to **$93.5 billion** (Stanford AI Index 2022). **Nearly 80%** of everyday devices now employ some form of AI (Neurosys 2022). McKinsey has predicted AI could deliver "an additional global economic output of about $13 trillion by 2030, boosting global GDP by about 1.2 percent a year." (McKinsey AI in Government 2022).

The disruption and potential risks of AI are increasingly the focus of regulators around the world. And for good reason. AI is different in many respects from past technological iterations and disruptions: AI is difficult to understand, challenging to oversee, adaptable and influential. As the US Department of Commerce's National Institute for Standards and Technology just pointed out in its long-anticipated, congressionally mandated risk framework, AI is "a uniquely challenging technology to deploy and utilize both for organizations and within society," with at least 14 distinct types of risk "that are not comprehensively addressed by current risk frameworks and approaches."

Further, AI systems aren't limited to chatbots and image generation systems. AI is increasingly being used in critical systems from defense to healthcare to financial services. As a result, AI has the ability to amplify benefits and risks throughout key industries at enterprise scale. One healthcare AI with discriminatory outputs was deployed in a system covering hundreds of millions of patients.

At the same time, disclosure by public companies regarding the use and influence (and attendant risks) of AI within their businesses remains limited. As the use and influence of AI grow in significance, companies may need to consider the resultant impacts on their businesses from economic, regulatory, risk management and control perspectives and provide appropriate public disclosures regarding the same.

What is AI?

Artificial Intelligence (AI) is notoriously hard to define. As the World Intellectual Property Organization (WIPO) observed: "There is no universal definition of artificial intelligence (AI)." The National Science and Technology Council agreed: "There is no single definition of AI that is universally accepted by practitioners." Indeed, deep into the deliberations over the EU's new AI regulation, first among the "outstanding issues" was "the definition of an AI system." And the current definition in that Act remains wide enough to swallow any number of unintended traditional software applications, with such catch-all terms as "statistical" and "logic-based" approaches, as well as "search methods." In other words, the most prominent and advanced draft regulation of AI is still grappling with how to workably define the technology.

A useful and simple introductory definition of AI is, in the words of AI pioneer Alan Turing, "thinking machines" (or perhaps "learning machines") — that is, machines or software that have the ability to solve problems with some degree of freedom, ingenuity, and adaptability, sometimes in ways that are surprising or even unexplainable to humans who make, use and rely on the technologies. Such an understanding can go a long way toward capturing what distinguishes AI from traditional software in common parlance. The EU has helpfully noted what AI is not, drawing a distinction against traditional software and noting that a "system that uses rules defined *solely* by natural persons to *automatically* execute operations should not be considered an AI system." (emphasis added).

More formal definitions of AI vary widely, however, with real consequences for the scope and nature of regulation. On the one hand, broader definitions aim to future-proof AI regulation but do so at the risk of capturing standard technologies that bear little resemblance to a core understanding of AI and its risks and benefits. For example, an early and oft-cited definition by John McCarthy describes AI as "getting a computer to do things which, when done by people, are said to involve intelligence." As AI researchers have since noted, a calculator could satisfy such definitions. CSIS likewise notes that "computer systems that in their heyday were routinely called 'AI,' such as IBM's chess-playing Deep Blue system in 1997, have higher-performing successors today that are merely called 'software' or 'apps.' Such observations have led to another common aphorism among AI experts: AI is whatever we haven't invented yet."

Other definitions focus on the broad aims of AI rather than its methods: *ie,* to make recommendations or solve problems. The National Artificial Intelligence Act of 2020 states (tracking OECD's definition): "The term 'artificial intelligence' means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments." But once again, many routine functions would be captured here, despite shifting the emphasis from means to ends. Traditional software follows human-defined objectives and provides outputs (*ie,* "decisions" or at least "recommendations"). And ironically it is AI, not traditional software, that could one day to discard human-defined objectives. The modifier "human-defined" was temporarily removed from the EU's working description of AI systems in April, though it appears in the current July draft. As NIST noted, with restraint that may one day seem quaint: "AI systems are designed to operate with varying levels of autonomy."

Narrower definitions of AI, which often focus on specific "AI" technologies of the day, seek to avoid definitions that are "ambiguous and too broad," and in so doing, run the risk of capturing too little, as technology outpaces legislation. The latest EU compromise language on AI "narrows it down to systems developed through machine learning techniques and knowledge-based approaches," and adds specific enabling powers for the Commission to "to adopt implementing acts to further specify and update techniques" to remain "flexible and future proof." Likewise, Section 238 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 lists current AI technologies like "cognitive architectures and neural networks" in its definition, while hedging with broad catch-all's. It remains to be seen whether such belt-and-suspender definitions get the best or worst of both worlds.

Other definitions focus on central *qualities* of AI, such as its ability to "learn" from data, particularly iteratively and adaptively, improving over time with new information and possibly limited human oversight. Microsoft Azure explained: "Artificial Intelligence is the ability of a computer system to deal with ambiguity, by making predictions using previously gathered data, and learning from errors in those predictions in order to generate newer, more accurate predictions about how to behave in the future."

This generative view still references traditional tools, from statistical modeling (with "ambiguity" serving as a close cousin to "uncertainty," driving the need for "predictions") to adaptation through feedback loops. But what this approach captures nicely is the ability of these tools, compiled in increasing levels of complexity, to take on the appearance of emergent ingenuity, autonomy, and learning. A weathervane is a system that changes direction with new inputs, but AI changes its own vast and unintelligible engine while we are expected to hop on for the ride. The question then becomes not what AI is, but how much influence does it have (*ie,* how much control and understanding do humans lose in the process, and over what values)? That is a definition with regulatory import. And that may be the heart of the matter, because at the end of the day, the reason AI elicits such attention separate and apart from the tools that compose it is the possibility – or probability – that these systems become so complex, evolving, influential, and autonomous that we cannot understand (or control) them, yet also too superior to human skills to ignore or override.

The White House may have come closest to this impact-based approach in its Blueprint for an AI Bill of Rights. While this document is non-binding (and not even a Bill of Rights yet, but a "blueprint" for one), it wisely casts a wide net reaching past the *type* of technology and aiming its regulatory focus on a unique set of *impacts*: "This framework applies to (1) automated systems that (2) have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services." As NIST also noted, AI has the ability to impact these values *more*. As the White House concluded, "These rights, opportunities, and access to critical resources of services should be enjoyed equally and be fully protected, regardless of the changing role that automated systems may play in our lives."

It is no surprise the world is struggling to define AI. We can scarcely define human intelligence, much less its artificial varietal. No definition is perfect, and time, regulation, and litigation will bear out which definitions are most useful and usable in each specific context. Yet thinking about AI, in simple terms, as a technology that shifts the traditional human/tool relationship – the balance of power and division of responsibility in vital areas – helps to assess risks and benefits.

Regulation and oversight

Prominent figures in technology and geopolitics have stressed the potential dangers of AI, with varying degrees of urgency and provocation. Stephen Hawking famously said that the "development of full artificial intelligence could spell the end of the human race," noting it "would take off on its own, and re-design itself at an ever increasing rate. Humans, who are limited by slow biological evolution, couldn't compete, and would be superseded." By "full" artificial intelligence (sometimes called "general" or "strong" AI), Dr. Hawking described a stage of development or advancement beyond simply solving pre-defined problems to broad awareness and reasoning, or as Henry Kissinger put it, AI that "establishes its own objectives." Speaking directly to that broader notion of AI, Elon Musk predicted: "[t]he risk of something seriously dangerous happening is in the five-year time frame. 10 years at most." Calling for oversight, Musk stated, "Mark my words, AI is far more dangerous than nukes. Far. So why do we have no regulatory oversight?" As Kissinger wrote in 2018, "The United States has not yet, as a nation, systematically explored [AI's] full scope, studied its implications, or begun the process of ultimate learning." The current pace of AI advancement continues to make difficult a deep understanding of its fullest embodiments.

History also has not been kind to those who predict the pace of AI's evolution. Referring to autonomous vehicles, the Guardian predicted in 2015 that "from 2020 you will become a permanent backseat driver." Others have erred on the side of overestimating AI progress. In early 2017, Oxford surveyed 352 AI experts to predict certain AI milestones, such as beating a human at the Chinese game Go. The average prediction was 2027 – it happened a couple months later in March 2017. Reactive regulation that underestimates the pace of AI innovation and influence poses a significant risk.

The number of proposed and developing frameworks for the regulation of AI is substantial. OECD maintains a live repository of "over 700 AI policy initiatives from 60 countries, territories and the EU." They span US Executive Orders like Maintaining American Leadership in Artificial Intelligence to national and regional policies and proposed legislation from AI frontrunners US, China, UK, Israel, dozens of nations, and international cooperation including US bilateral commitments and work with the G7, G20, OECD, Global Partnership on AI (GPAI), and the UN, including an ethical AI policy signed by all 193 members of UNESCO, as well as a patchwork of emerging state laws. Consolidation and harmonization of these regulatory initiatives could help to provide clarity and predictability.

Certain patterns are emerging, with a fairly consistent set of "human-centric" AI values including privacy, security, safety, transparency, human oversight, and fairness, as well as calls for corporate operational AI controls, self- and third-party design and impact assessments, data quality controls and governance, and the eradication of malicious and biased AI use. In October 2022, the White House released its non-binding 73-page Blueprint For An AI Bill of Rights, describing AI-related technologies as one of the "great challenges posed to democracy today" and articulating five guiding principles "to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence." These are (1) safe and effective systems, (2) algorithmic discrimination protections, (3) data privacy, (4) notice and explanation, and (5) human alternatives, consideration, and fallback.

A current and urgent focus (see also here and here) of regulatory efforts is the ability of even "neutral" algorithms to amplify and scale discrimination in access to vital goods, services, and rights, including banking, housing, healthcare, and employment. Many approaches recognize that a risk-based regulatory structure is needed as one-size-fits-all schemes are less likely to adequately address a field as broad and fast-paced as AI.

There are notable exceptions, however. The FDA's September 2022 Final Guidance on Clinical Decision Support Software removed its prior reliance on the International Medical Device Regulators Forum (IMDRF)'s risk categorization framework, opening a broad swath of low-risk devices already on the market to regulatory review.

Also, the EU's proposed AI Regulation is aspiring to be the first horizontal, broad-based AI law, with extraterritorial reach over "providers placing on the market or putting into service AI systems in the Union." The proposed rule would distinguish forbidden uses (such as deep fakes and subliminal manipulation), high-risk AI (for both regulated sectors and human services affecting key rights), and limited-risk AI. High-risk AI would be subject to conformity assessments and required controls, while limited-risk AI would have transparency requirements. Violations of the proposed law could carry substantial fines (up to the *greater* of €30 million or 6 percent of global turnover), on top of GDPR penalties. The potential complexity and reach of the EU proposal has led some to characterize it as GDPR 2.0.

Proposed legislation in the US has been narrower, focused largely on protecting access to vital goods, services, and rights and the elimination of AI's ability to amplify and scale discrimination. On this topic, the US and EU approaches have similarities. The American Data Privacy and Protection Act (ADPPA) would address algorithms "making or facilitating advertising for, or determining access to, or restrictions on the use of housing, education, employment, healthcare, insurance, or credit opportunities," as well as access to public accommodations and any "disparate impact on the basis of individuals' race, color, religion, national origin, sex, or disability status." The EU's list would include credit assessments, recruiting and employment, criminal justice, and most recently, systems affecting children, insurance, medical triage, and democracy including voting. The US law would also require design and impact assessments for covered entities and expressly enable enforcement by FTC. State and local regulators, from Colorado's Division of Insurance to New York City's Department of Consumer and Worker Protection, are promulgating anti-bias rules across sectors and mandating AI anti-bias audits.

Another important variable in many proposed and existing regulations is the level of autonomy afforded to AI systems. The issue is particularly salient in the defense industry, such as regulations related to Lethal Autonomous Weapon Systems (LAWS), *ie,* weapons programmed to make targeting and kill/no-kill decisions without human intervention. The Congressional Research Service (CRS) described them as "a special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ an onboard weapon system to engage and destroy the target without manual human control of the system."

There is currently no international or domestic ban on such weapons, and some – like autonomous cyber weapons – are exempted from existing policy. Existing regulations focus on flexible, risk-based case-specific uses, largely turning on the degree of human control versus the nature of the potential harm. Department of Defense Directive (DODD) 3000.09 instructs that autonomous and semi-autonomous weapons systems "shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force." In other words, CRS notes, there is not "a fixed, one-size-fits-all level of human judgment that should be applied to every context. What is 'appropriate' can differ across weapon systems, domains of warfare, types of warfare, operational contexts, and even across different functions in a weapon system." Common LAWS parlance distinguishes human-in-the-loop systems (in which a human must confirm an attack), on-the-loop systems (in which a human can veto a proposed attack), and off-the-loop systems (which are fully autonomous and proceed without human control). But as many have noted, DODD 3000.09 was drafted in 2012 and does not specifically address AI per se. Updates for "AI-enabled" weapons may come soon.

Within the transportation industry, NTHSA has defined 6 levels of autonomy for vehicles, from Level 0 (Momentary Driver Assistance) to Level 3 (Conditional Autonomation) to Level 5 (Full Automation, not expected until 2025+). Level 3 denotes a system that is autonomous, but the human driver retains full ability to take over at any point. These designations carry weight for liability and the distribution of risk between manufacturer and consumer. For instance, Level 2 instructs humans: "You Drive, You Monitor," admonishing "you, as the driver, are responsible for driving the vehicle." Level 3, by contrast, requires that the human is "available to take over driving *if requested*" by the vehicle (emphasis added). And by Level 4, the vehicle is "fully responsible for driving tasks within limited service areas while occupants act only as passengers and do not need to be engaged." While Level 3 and 4 technologies are not yet available to US consumers, it is not hard to see the gradations in responsibility that the tort system may assign to these varying levels of control. For now, NTHSA states: "Every vehicle currently for sale in the United States requires the full attention of the driver at all times for safe operation." That has not stopped litigation over allegations of so-called phantom braking, failed lane-keep assist, and other semi-autonomous assistive technologies in the US and abroad.

Biomedical and healthcare leaders have similarly described relevant levels of autonomy in medical devices. The American Medical Association has described two levels, "assistive" and "autonomous," and argued that AI should be recharacterized as "Augmented Intelligence," not "Artificial Intelligence," to affirm the pivotal role of the doctor in the chain of healthcare delivery, standing between device and patient. FDA has identified three levels of autonomy, asking whether software "informs," "drives," or directly "diagnoses" / "treats" a patient.

FDA has incorporated additional factors in its analysis of AI regulation, including the level of seriousness of the condition to which the AI is being applied. This creates a 3x3 grid with nine boxes, which in turn reflect four distinct levels of regulatory focus. With increased granularity comes more precision in the sort of case-specific analysis supported by DOD and FDA, but also more complexity. The question, to be tested empirically, is whether this brings more or less regulatory predictability and efficiency. The issue of bias in medical AI is receiving intense scrutiny, with pending HHS policy on the horizon that could impose significant obligations on users of medical AI.

Another common debate in regulation of AI is the level of "explainability" required, or put simply, can a human understand why a machine reached a certain decision? The Consumer Financial Protection Bureau (CFPB) recently clarified in Circular 2022-03 that the Equal Credit Opportunity Act (ECOA) and Regulation B require creditors "to provide a statement of specific reasons to applicants against whom adverse action is taken," prohibiting them from using complex "black box" (unexplainable) algorithms "when doing so means they cannot provide the specific and accurate reasons for adverse actions."

And yet explainability is not a one-size-fits-all solution: in some instances, the need for greater speed or accuracy may justify black box solutions. FDA exempts from regulation clinical decision support software that "informs" medical providers (the lowest level of reliance) if the recommendations are explainable (or, in FDA's words, where the provider can "independently review the basis for such recommendations"). FDA nonetheless permits black box algorithms, subject to regulatory clearance, recognizing that in some cases, opaque AI may offer better health outcomes than explainable AI or clinicians alone.

Likewise, DODD 3000.09 generally requires that weapons systems be "readily understandable to trained operators" and "provide traceable feedback on system status." Yet certain systems, including missile defense, are exempt from 3000.09, and even under that directive, the requirement for human oversight is limited to what is "appropriate" under the circumstances.

Whatever the final form of applicable regulations may be, companies should prepare now for both general and industry-specific regulation across jurisdictions, with baseline "human-centric" AI values of privacy, safety, security, transparency, fairness, reliability, and, where appropriate, explainability and human oversight. Special attention should be paid to AI in highly regulated industries, in which new AI rules must mesh with existing regulations, as well as industry-agnostic AI which have the ability to affect access to vital goods, services, and rights.

Litigation and enforcement

As standards evolve, enforcement and litigation regarding AI are growing and important trends are emerging. First and foremost, agencies across the Executive Branch have sought to demonstrate that AI enforcement can and will occur under existing statutes, notwithstanding efforts to specify or broaden those abilities. The FTC has asserted its jurisdiction over AI, noting that its mandate to curtail "unfair or deceptive practices" under the existing regulations "would include the sale or use of – for example – racially biased algorithms." The FTC has also invoked the Fair Credit Reporting Act and the Equal Credit Opportunity Act, which "makes it illegal for a company to use a biased algorithm that results in credit discrimination."

Likewise, the CFPB recently called for AI whistleblowers, noting AI "technologies can help intentional and unintentional discrimination burrow into financial decision-making systems, and whistleblowers can help ensure that technologies are applied in law-abiding ways." A recurring theme is the applicability of old laws to new technology. Describing its "first criminal prosecution against a conspiracy specifically targeting e-commerce," the DOJ's Antitrust Division stated in 2015: "We will not tolerate anticompetitive conduct, whether it occurs in a smoke-filled room or over the Internet using complex pricing algorithms."

Several enforcement actions have centered on the acquisition and use of the data that educates and informs AI. In 2019, the FTC settled claims related to allegations stemming from the use of personal information for voter profiling and targeting. The FTC alleged "that app users were falsely told the app would not collect users' names or other identifiable information" when, in fact, the application collected User ID connected to their profiles. Notably, the settlement required the company to delete not only the ill-gotten information but "any information or work product, including any algorithms or equations, derived in whole or in part from" that data. This penalty would come to be known as algorithmic disgorgement or model destruction, resulting in loss of AI systems that were trained or validated on unauthorized data. FTC Commissioner Slaughter wrote in the *Yale Journal of Law & Technology*: "This innovative enforcement approach should send a clear message to companies engaging in illicit data collection in order to train AI models: Not worth it."

In 2021, the FTC approved a settlement with a photo app developer of claims respecting its use of facial recognition technology and retention of photos and videos. The FTC required that, before using any biometric information to "train, develop, or alter any face recognition model or algorithm," the company had to "Clearly and Conspicuously" disclose all purposes for which it would use or share that information "*separate and apart* from any 'privacy policy,' 'terms of use' page, or other similar document" (emphasis added), then obtain affirmative consent from US users. "Clearly and Conspicuously" was a defined term with eight elements. The FTC again required the company to delete "the models and algorithms it developed by using the photos and videos uploaded by its users." In March 2022, FTC extended its use of algorithmic disgorgement to an action brought under a federal privacy statute, the Children's Online Privacy Protection Act (COPPA), demonstrating its willingness to broadly apply the remedy.

Enforcement actions have also focused on algorithmic discrimination, both deliberate (disparate intent) and unintentional (disparate impact). In May 2022, the EEOC brought suit alleging violations of the Age Discrimination in Employment Act (ADEA) based on recruitment software that allegedly automatically rejected older applicants. EEOC Chair Charlotte A. Burrows stated: "This case is an example of why the EEOC recently launched an Artificial Intelligence and Algorithmic Fairness Initiative. Workers facing discrimination from an employer's use of technology can count on the EEOC to seek remedies." In June 2022, the DOJ announced a settlement of the "department's first case challenging algorithmic bias under the Fair Housing Act," resolving claims that a digital advertising system discriminated against users due to "algorithms [that] rely, in part, on characteristics protected under the FHA."

Regulators have also targeted fraud relating to AI. In 2021, the FTC settled claims against three companies that "allegedly used ticket bots to fool tests designed to prevent nonhuman visitors," resolving "alleged violations of the Better Online Ticket Sales (BOTS) Act."

Regulators have also enforced against the misuse of *other's* AI: In 2020, the Fraud Division of the DOJ imposed a fine of $920,203,609 relating to a trader who allegedly "traded in a manner to deceive other market participants that traded using automated trading systems or computer algorithms ("algos")." Notably, the trader was sanctioned for manipulating other peoples' AI, in his words using "a little razzle dazzle to juke the algos."

Regulators have targeted fraudulent claims *about* AI products: On June 28, 2022, the DOJ announced criminal charges against a cryptocurrency investment platform. Among other allegations, the indictment states the owner "falsely represent[ed] to victim-investors that he had personally developed and employed an Artificial Intelligence ('AI') trading robot (an 'AI trading bot')" that would "generate between 500% to 600% returns on the amount invested …. But, in fact, there were no profits because [defendant] did not have an AI trading bot." Trial is currently set for 2023. The case is a good reminder to make realistic claims about new technologies, or, as that US Attorney put it, not to "hide behind trendy buzzwords" when "seeking to separate people from their money."

Enforcement activity has also arisen related to the unauthorized use of AI in highly regulated industries like healthcare. In 2018, the FDA sent a warning letter alleging that a company had marketed an adulterated and misbranded product. The FDA claimed that the company had gone "significantly beyond" its clearance to offer radiologists "an electronic platform, with basic image-processing functionality" by "utilizing machine learning algorithms to automatically detect and mark abnormalities on medical images." The FDA premised this claim on the basis that "providing computer-assisted detection (CADe)" was not supported by the original clearance. The FDA warned: "The lack of evidence demonstrating the safety and efficacy of [these] automatic detection and characterization capabilities raises public health concerns. Specifically, the risks for the device as advertised are low sensitivity and specificity (*ie,* the device has unknown false positive and false negative rates)." In 2019, the FDA sent a closeout letter to the company, noting "[f]uture FDA inspections and regulatory activities will further assess the adequacy and sustainability of these corrections."

Similar trends are emerging in private litigation. In 2016, a putative class action alleged that an app had restricted price competition. Litigation has also focused on biometrics and privacy. In 2021, a company settled a class action for $650 million over allegations that its facial recognition software violated the Illinois Biometric Information Privacy Act. Another putative class accused an insurer of using facial recognition tools without consent regarding AI tools that searched customer videos for "non-verbal cues" and "signs of fraud." Among other causes of action, plaintiffs asserted breach of contract claims and GBL § 349 claims of deceptive acts, which both survived a motion to dismiss.

Numerous claims have pursued theories of discrimination, civil rights violations, and deprivation of due process resulting from algorithmic decisions. On March 18, 2022, a private litigant brought putative class action under the Equal Credit Opportunity Act, alleging that a financial services company used "automated algorithms and machine learning to make underwriting decisions" that "singled out predominately Black neighborhoods and labeled those neighborhoods ineligible for rapid processing." In another matter, the Michigan Supreme Court affirmed that plaintiffs could seek monetary damages for due process violations where the state used a fraud-detection algorithm to deny unemployment benefits without meaningful notice or an opportunity to be heard. As employers increasingly adopt AI-enabled recruiting and hiring tools, Verisk has estimated that "economic losses from claims based on algorithmic hiring biases are expected to be

USD 3 billion over the next 10 years and non-economic losses – from punitive damages and legal costs, for example – could easily be orders of magnitude higher, according to research from AIR."

Among product liability claims, cases involving accidents with autonomous vehicle cases are regularly brought. Recently, a spate of product liability cases have focused on the issue of algorithms propagating allegedly harmful content, particularly with respect to children using platforms. The MDL petition involves nearly 50 different suits alleging injuries ranging from mental, emotional, and physical harm (in some cases, death) caused by use of social media platforms, which many plaintiffs claim are designed to be addictive and therefore unreasonably dangerous for children and teens.

The recent explosion of generative creative AI – which ingests the universe of existing arts and culture to spin out new variations with a range of a novelty – has also generated a predictable progeny of IP-related AI litigations. Artists have sued to allege copyright infringement (with Nick Cave, not a litigant at the time of publication, calling AI-generated songs "in the style of Nick Cave" a ""a grotesque mockery," noting "as far as I know, algorithms don't feel." At the same time, AI enthusiast Dr. Stephen Thaler is at the lip of the Supreme Court, contesting the Federal Circuit's view that only humans can be inventors under the Patent Act.

While these early disputes may be provocations and curiosities, companies across the nation are grappling with employees using generative AI to create new content, from product ideas to reports to art design, with or without employer knowledge, portending a spate of infringement claims and producing a novel category of Generative AI Policies.

The SEC and AI

The SEC has not proposed prescriptive regulations or provided tailored guidance regarding AI-related disclosures, but the SEC has recognized the potential and risks of AI technology. The SEC itself has also embraced the use of big data and AI technology.

The SEC has required certain data to be presented in machine-readable format since 2003 (for Section 16 filings) and in 2018, the SEC adopted rules requiring companies to use inline eXtensible Business Reporting Language (XBRL) for certain information, including financial statement information.

"Big data" is instrumental to the Division of Economic and Risk Analysis or DERA, the SEC's financial economics and data analytics division created in September 2009. Additionally, AI is one the SEC's Strategic Hub for Innovation and Financial Technology (FinHub)'s four areas of attention- the other three areas are: 1) blockchain/distributed ledger; 2) digital marketplace financing; and 3) automated ("robo") investment advice, which the SEC discussed in connection with AI at their March 10, 2022 Investor Advisory Committee meeting.

In October 2016, at the Midwest Region Meeting for American Accounting Association (AAA), then-Acting Director of DERA Scott W. Bauguess described how the SEC was adopting machine learning to assess market risks, and noted that in a world of "big data," machine learning is becoming more advanced and expanding in potential.

In a 2017 keynote address titled "The Role of Big Data, Machine Learning, and AI in Assessing Risks: A Regulatory Perspective," Director Bauguess discussed AI's impact on our daily lives and the remarkable advancements of AI, noting the challenge for regulators created by the complexity of AI and the vast amount of data that is input into any decision an algorithm makes. He also acknowledged that, while AI is a remarkable technology, it comes with serious risks such as unobservable outcomes, fraud, unreliability of data, the dependence on skilled workers and challenges processing and understanding structured and unstructured data.

In 2019, then Chief Economist and Director of DERA S.P. Kothari discussed AI-related challenges at the Big Data and High-Performance Computing for Financial Economics, National Bureau of Economic Research. Some challenges he noted included maximizing the security of confidential information, maintaining the technology and workforce to stay ahead of big data developments and communicating meaningfully and effectively with stakeholders.

Analysis of AI-related disclosures

To date, AI-related disclosures by public companies have been limited, and primarily relate to risks associated with AI technology generally and, to a lesser extent, descriptions of certain AI products and services, or competitive advantages related to the use of AI technology.

A. Artificial intelligence and machine learning risks

Regulation S-K, Item 105 requires companies to disclose the material factors that make an investment in the company speculative or risky. Item 105 directs registrants to concisely explain how each risk affects the registrant or the securities being offered.

A. STUDY OF AI-RELATED RISK FACTORS

A recent study by DLA Piper Corporate Data Analytics found that from July 2021-July 2022, a total of 71 public companies referenced 859 distinct risks related to AI in their Forms 10-K, 10-Q and registration statements. Approximately 36% of the disclosures were made by small cap issuers, 34% by medium-cap issuers and 30% by large cap issuers. Of the 71 companies disclosing AI-related risk factors, 52 were in the technology sector, 8 were in the financial services sector, 7 were in the healthcare sector and 2 were in each of the insurance and industrials sectors.

The most common categorical risks identified by sector were:

Technology

1. Reliance on third parties for data and technology and vendor non-compliance
2. Privacy
3. Reputational harm
4. Unpredictable or autonomous decisions/problems difficult to detect
5. Economic competitiveness
6. Inherent complexity and significant research and development expenditures

Financial Services

1. Reliance on third parties for data and technology and vendor non-compliance
2. Reputational harm
3. Inherent complexity and significant research and development expenditures
4. Data limitations and insufficiencies
5. Privacy

Healthcare

1. Reputational harm
2. Data limitations and insufficiencies
3. Privacy
4. Reliance on third parties for data and technology, vendor non-compliance
5. Open source AI risks
6. Social and ethical issues

Insurance

1. Privacy laws
2. Reliance on third parties for data and technology, vendor non-compliance
3. Reputational harm
4. Unintentional bias and discrimination and fairness
5. Inherent complexity and significant research and development expenditures

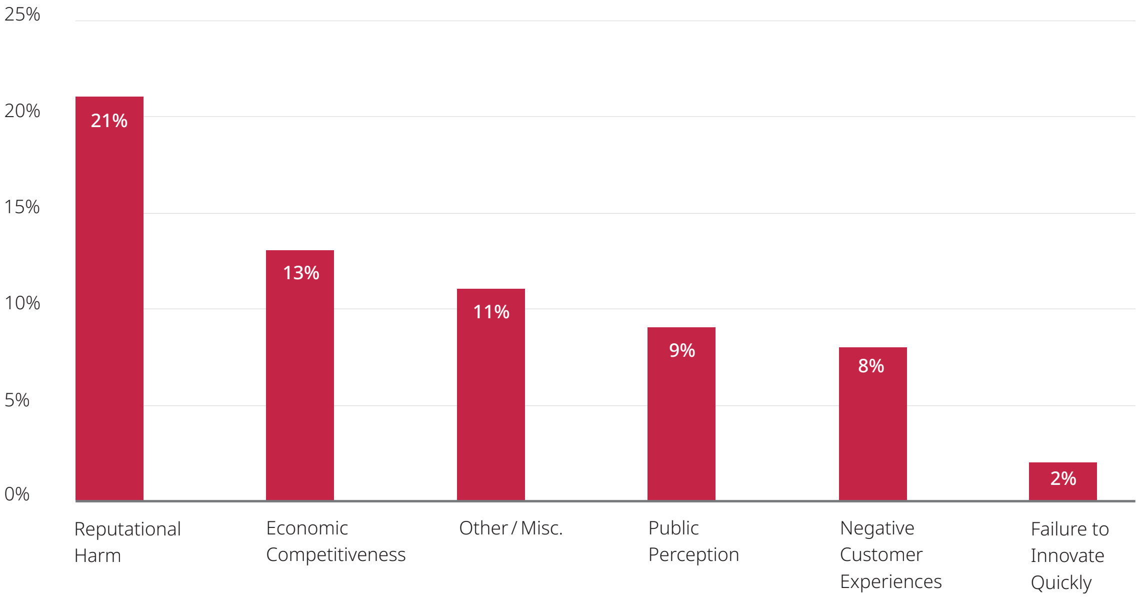
Industrials

1. Inherent complexity and significant research and development expenditures
2. Reliance on third parties for data and technology
3. Data limitations and insufficiencies
4. Open source AI risks
5. Privacy

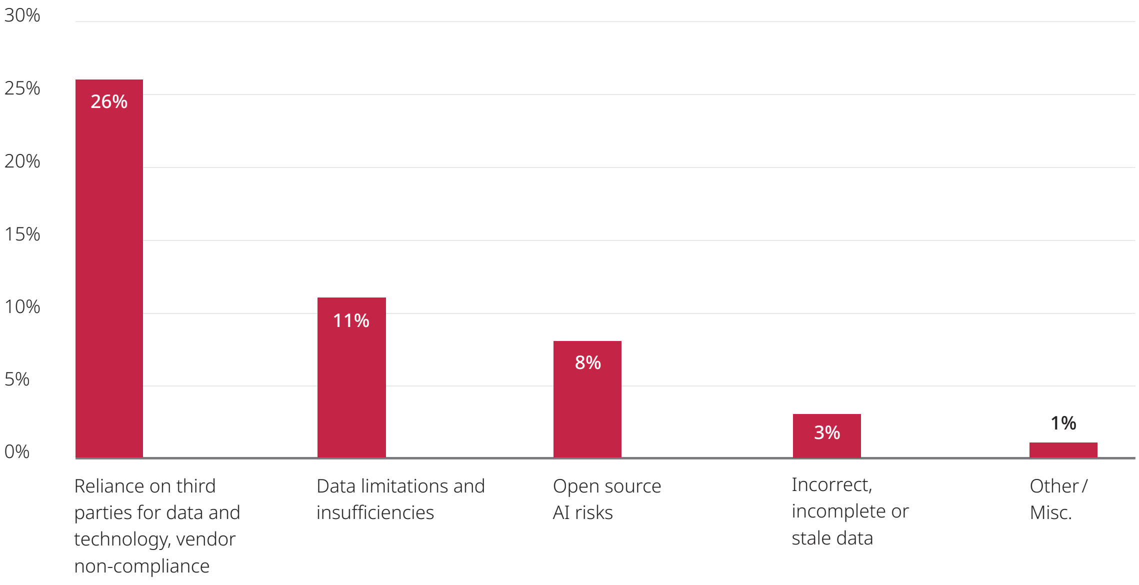
The below charts demonstrate the frequency of the most common risks mentioned in risk factors related to AI. With respect to each risk distinct risk, we present both (i) the percentage of all AI disclosures identified that reference that particular risk and (ii) the percentage of all AI disclosures found that reference that particular risk within a particular sector.

ANALYSIS OF IDENTIFIED RISKS BY ALL ISSUERS

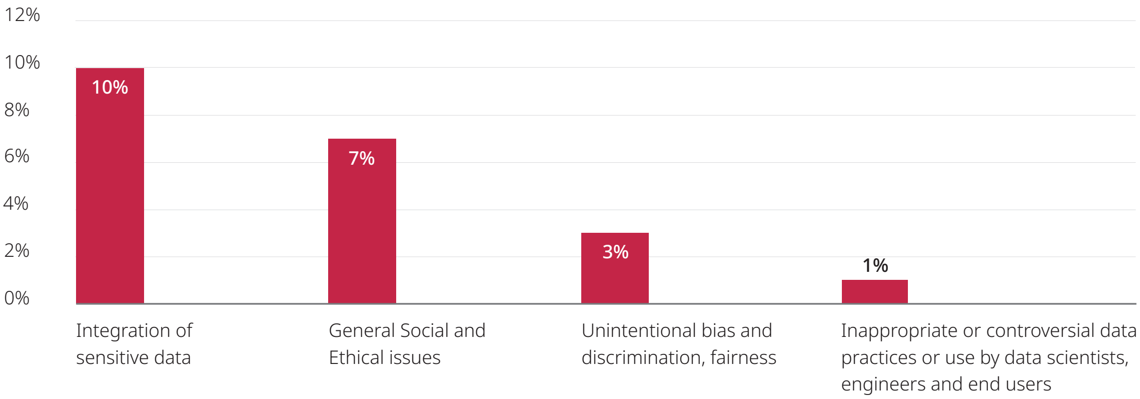
Deficiencies and Inaccuracies in AI Output and Reliability (All Companies)



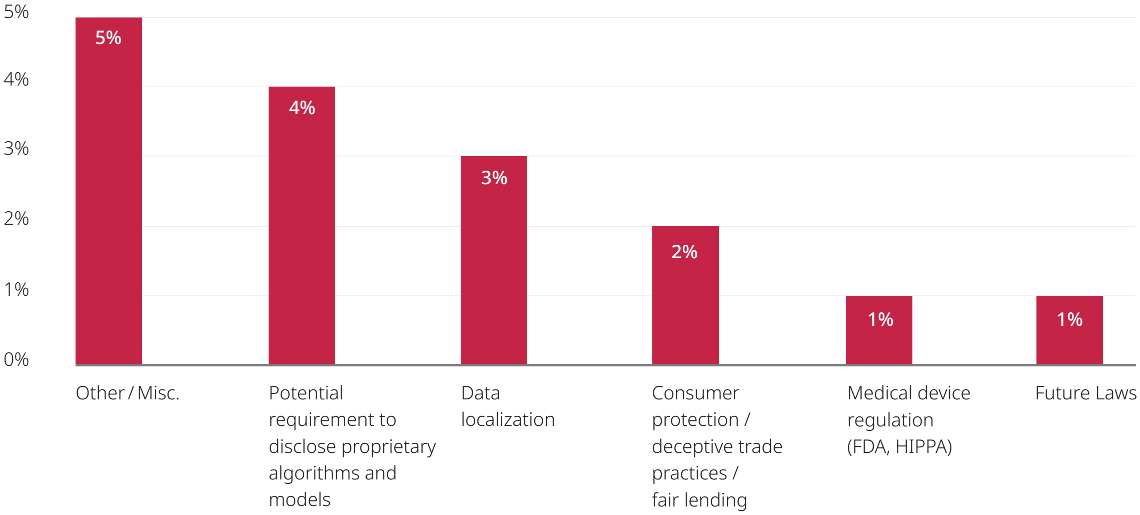
Dependence on and Flaws in Algorithms and Data Sets (All Companies, All Sectors)



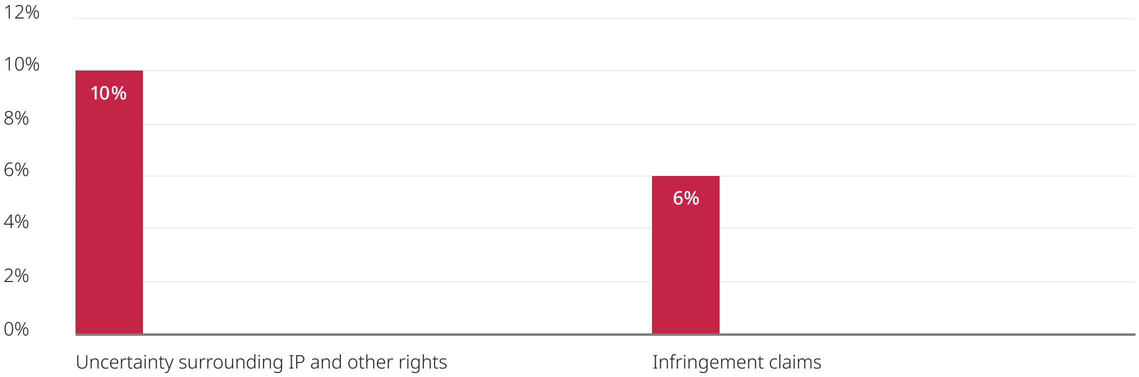
General Social and Ethical (All Companies, All Sectors)



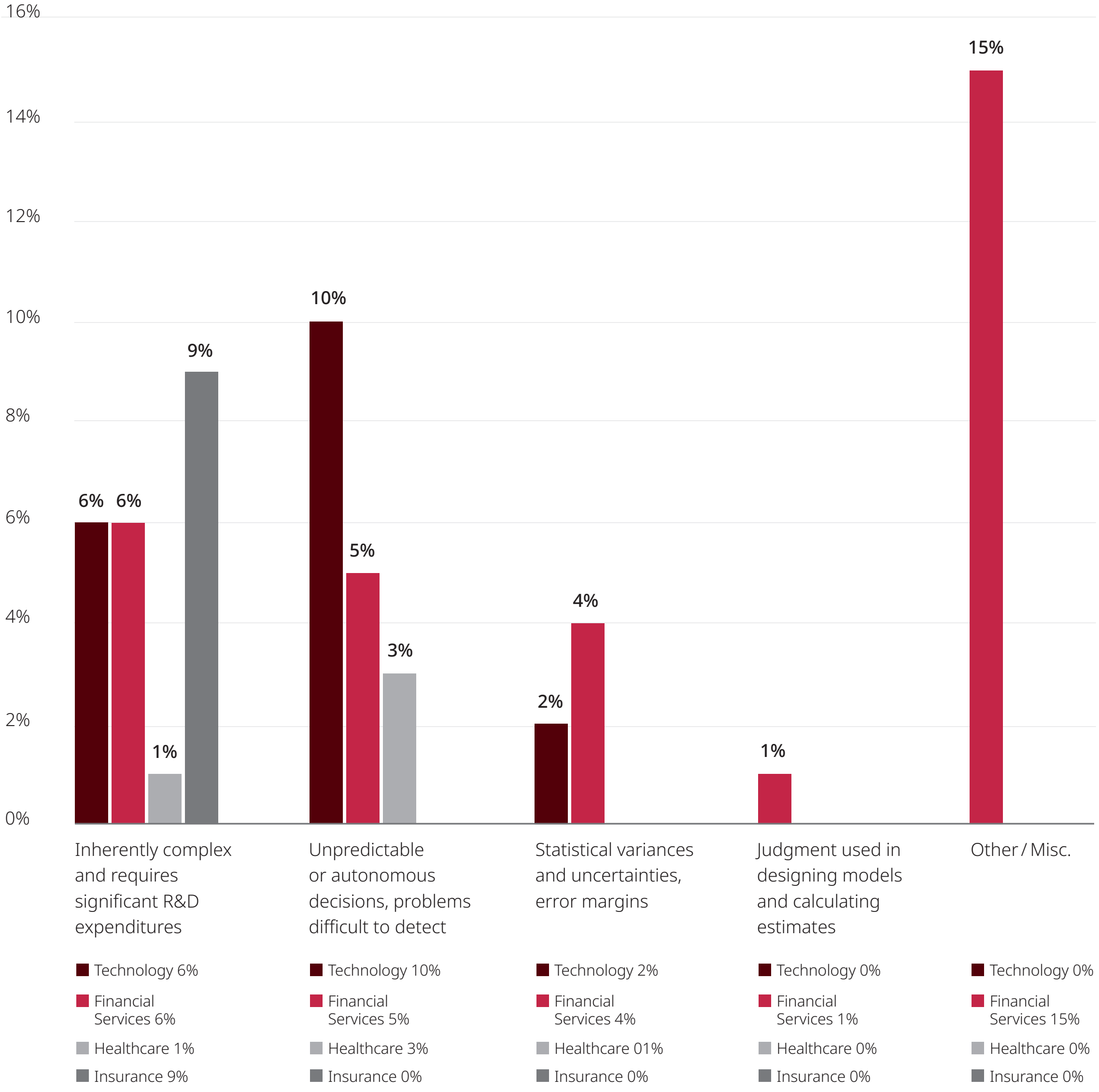
Increased Regulation, Investigation, Enforcement and Litigation – All Companies, All Sectors
(Other than Intellectual Property Disputes)



Intellectual Property Uncertainty and Infringement Claims (All Companies)



Deficiencies and Inaccuracies in AI Output and Reliability (Sector Analysis)

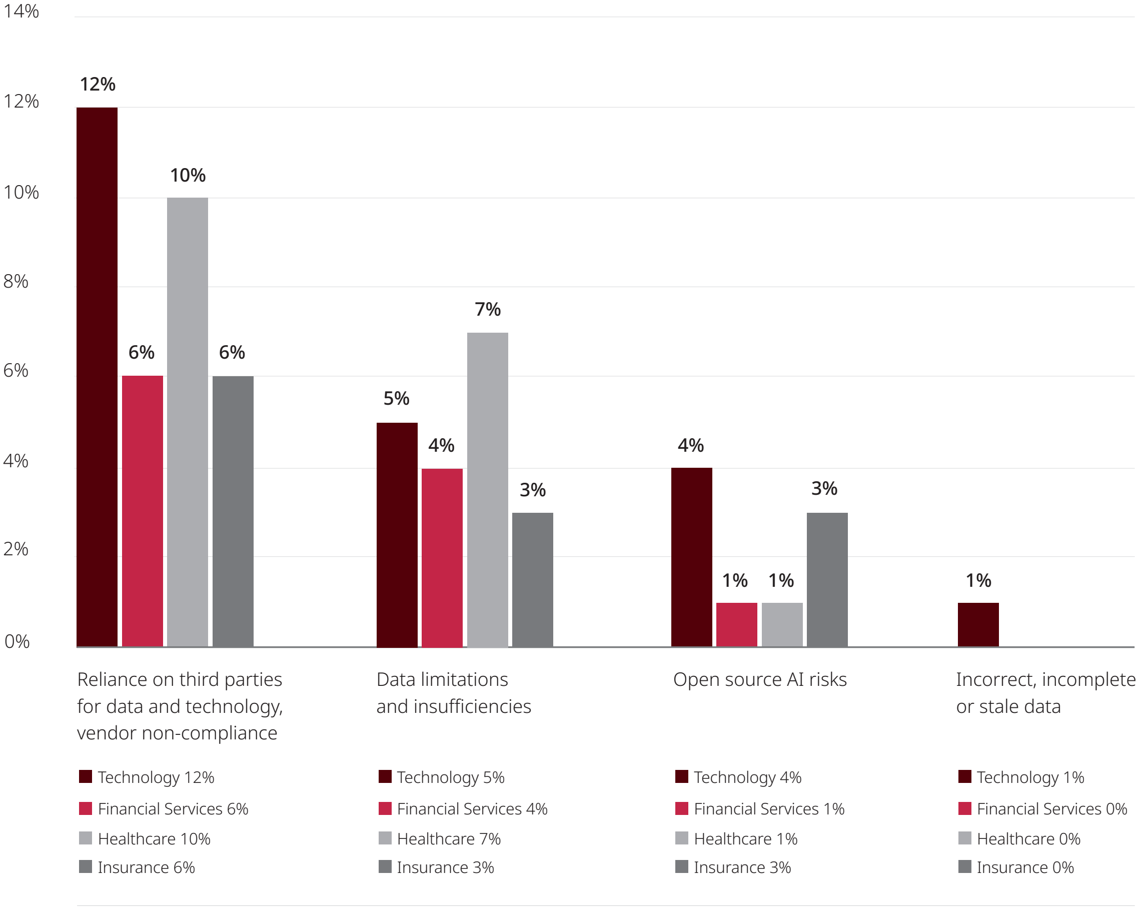


As demonstrated in the chart above, the issuers studied disclosed risks related to deficiencies and inaccuracies in AI output and reliability. The most common risk factor related to AI output and reliability is the inherent complexity of the technology and significant research and development expenditures required to support the technology.

Unpredictability and difficulty in identifying problems is the next most common risk factor that is seen in this category. Due to the nature of AI and machine learning, this technology may develop methods that were not foreseen and adopt operations that go against the original purpose of the product.

Statistical variances are also another commonly mentioned risk factor. If a company's product uses data that operates on statistically insignificant data, there is a risk for the product to produce misguided conclusions. In many cases, the process of data cleaning is a tedious and expensive task for companies to conduct. This risk can cause products to provide misguided solutions to customers and is an inherent risk due to AI reliance on data.

Dependence on and Flaws in Algorithms and Data Sets (Sector Analysis)

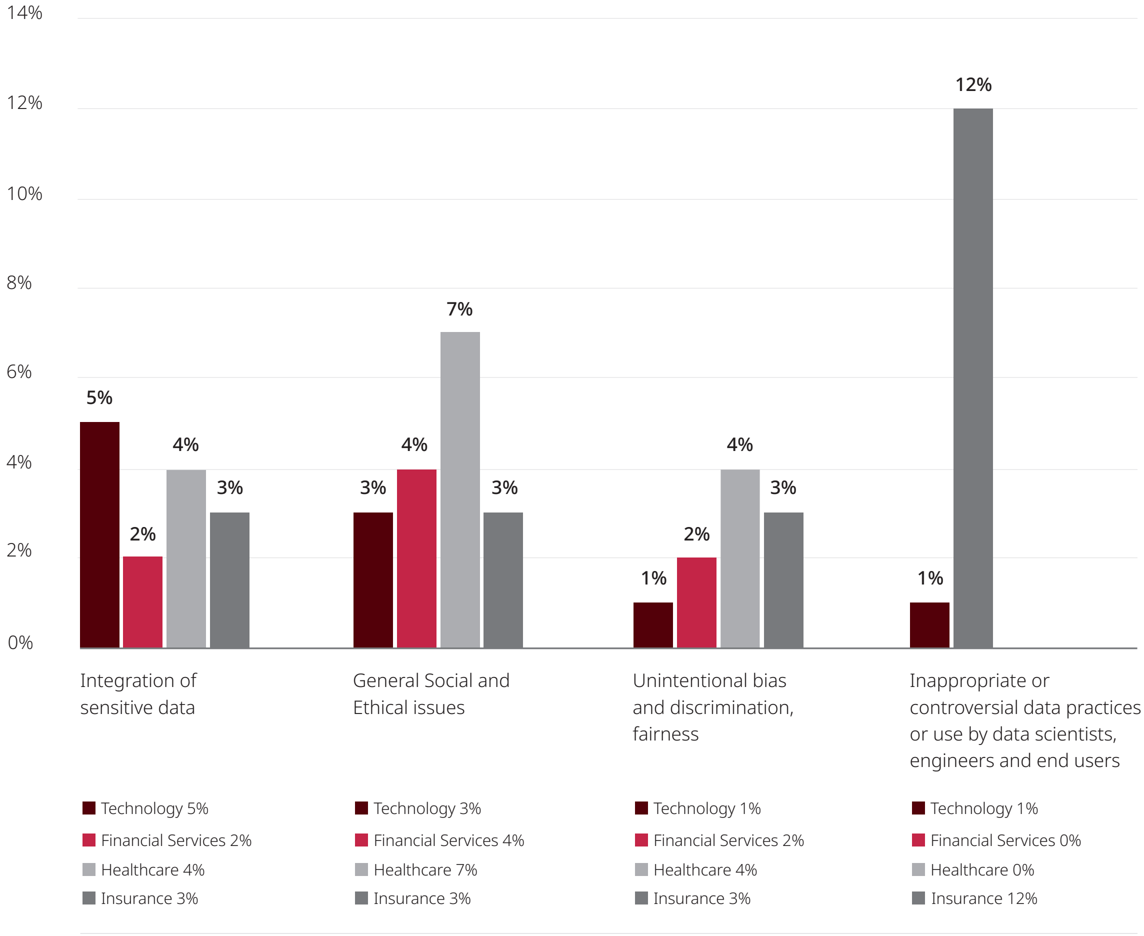


As demonstrated in the chart above, the issuers studied disclosed risks related to dependence on and flaws in algorithms and datasets. This chart shows that reliance on third parties is a commonly recognized risk within the aggregate sample. AI technology may be reliant on infrastructure as a service (IaaS) providers or other third parties, and issuers risk supply chain cyberattacks or outages.

Data limitations and insufficiencies are another rising risk amongst most industries. If data is insufficient, a machine learning product can be trained incorrectly and offer misguided solutions to consumers. Multiple outliers in a dataset may be mistaken as statistically significant if there is no data cleaning within an organization.

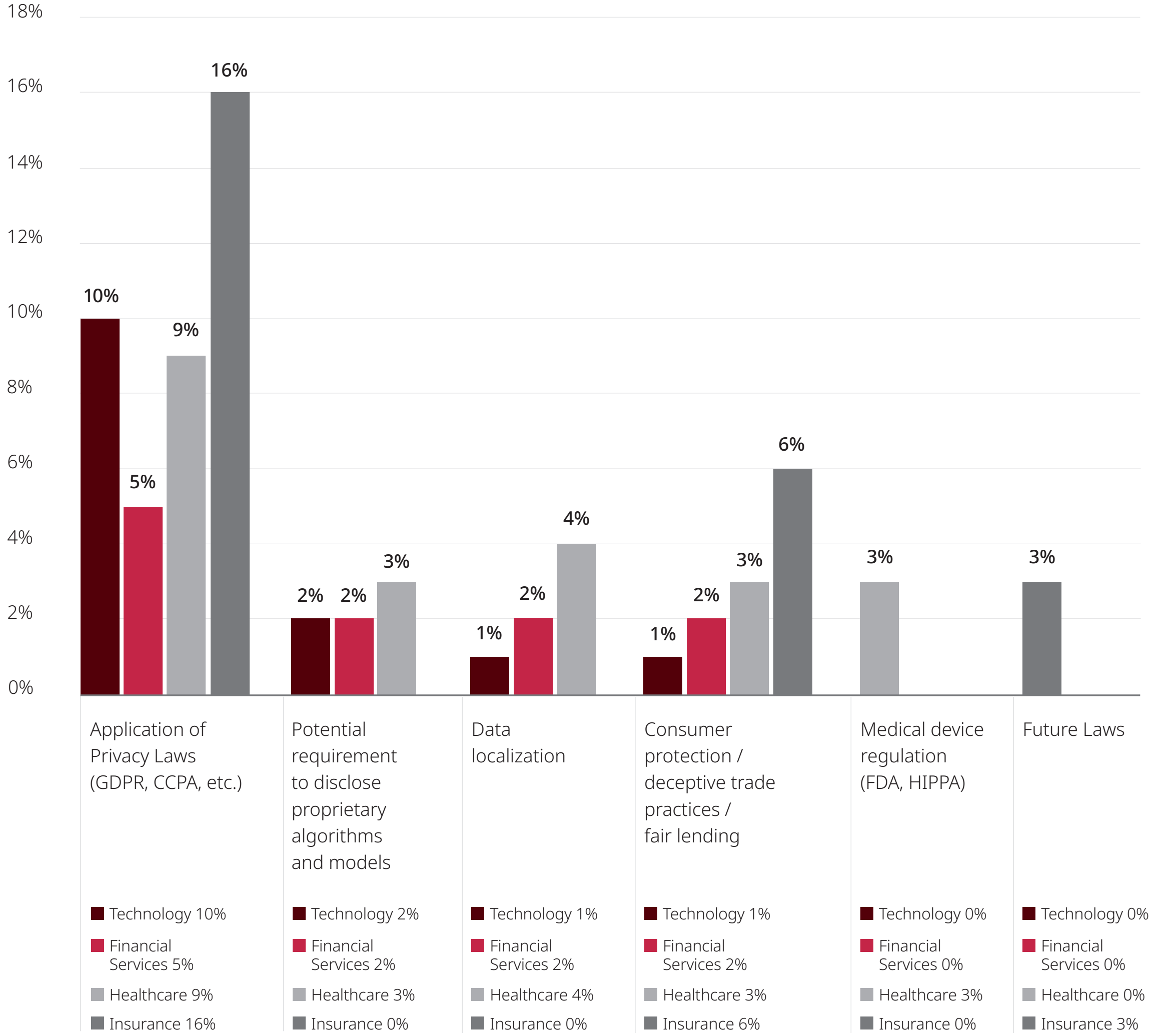
AI software is generally licensed by third-party authors that may use open source code. The use of open source code may restrict the functionality of companies' solutions or may require releasing the source code of certain applications. It also involves risks due to potential infringement claims, the lack of warranties in open source licenses, and the complexity in interpreting open source licenses due to the lack of precedent governing these licenses. Open source AI also may allow for more access to source code and allow bad actors to exploit security flaws within foundational software. While proponents of open source AI claim that increased transparency results greater detection of security flaws by allowing more individuals to manipulate the software, there is an attendant risk that those detecting the flaws are bad actors.

General Social and Ethical Issues (Sector Analysis)



As demonstrated in the chart above, the issuers studied disclosed risks related to social and ethical issues related to AI. The use of AI raises privacy, safety, employment, human rights and other social issues. The integration of sensitive data is a common risk factor amongst surveyed companies. Intrinsic flaws in AI algorithms and insufficient or biased information in datasets may result in unintentional bias affecting users, potential discrimination and controversial data practices. Stanford University's 2021 Artificial Intelligence Index Report found that diversity is a major challenge of AI technology, noting that only 2.4% of new US resident AI PhD graduates were African American and only 3.2% were Hispanic.

Increased Regulation, Investigation, Enforcement and Litigation – Sector Analysis
(Other than Intellectual Property Disputes)



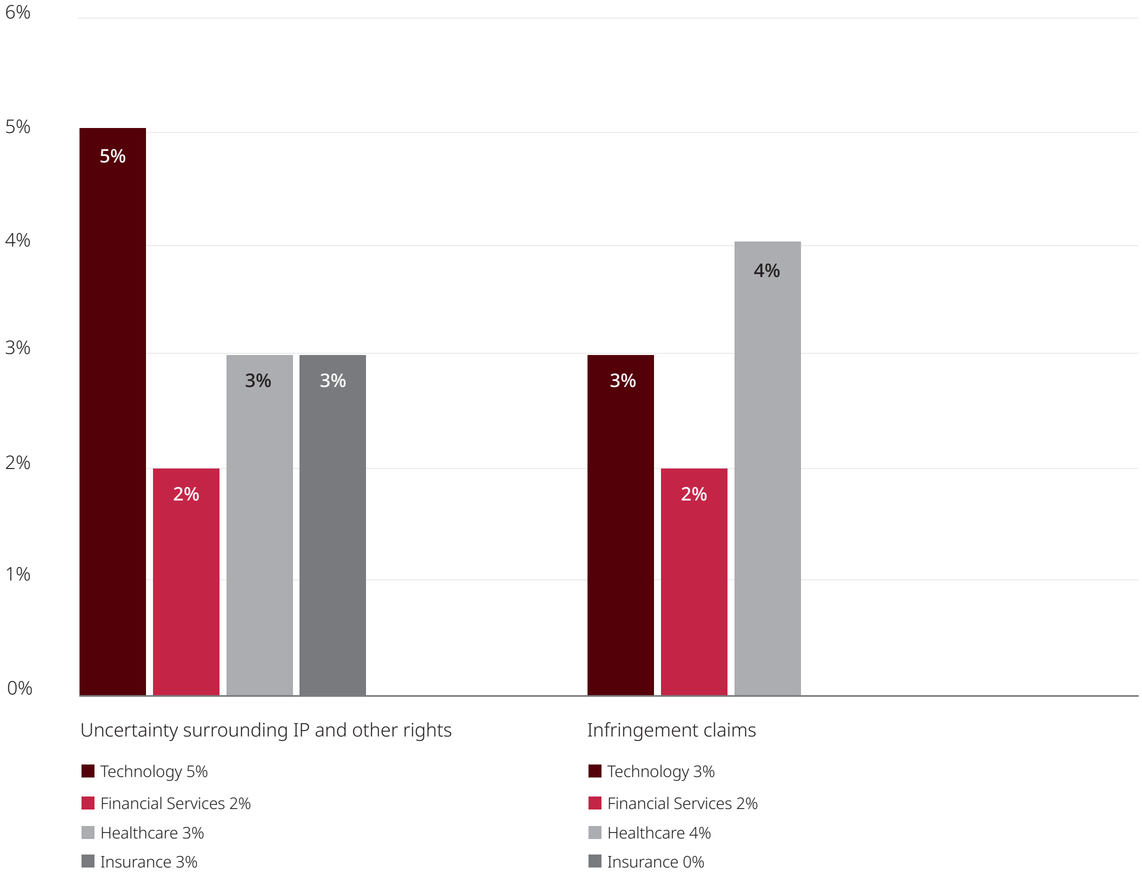
As demonstrated in the chart above, disclosing companies believe that the implementation of AI increases regulatory requirements and risks scrutiny from internal and external authorities.

This chart demonstrates that the application of privacy laws is one of the most common risk factors mentioned within the aggregate sample. This is the second most common risk factor out of all risk factors and is a rapidly developing area of regulation. In particular, 16% of insurance AI disclosures related to the risks associated with privacy laws.

Issuers in the technology, financial services and healthcare sectors noted the need to disclose proprietary algorithms and models. Due to transparency legislation, there may be requirements for companies to release their proprietary products which leaves them vulnerable to inadvertently sanctioned IP theft.

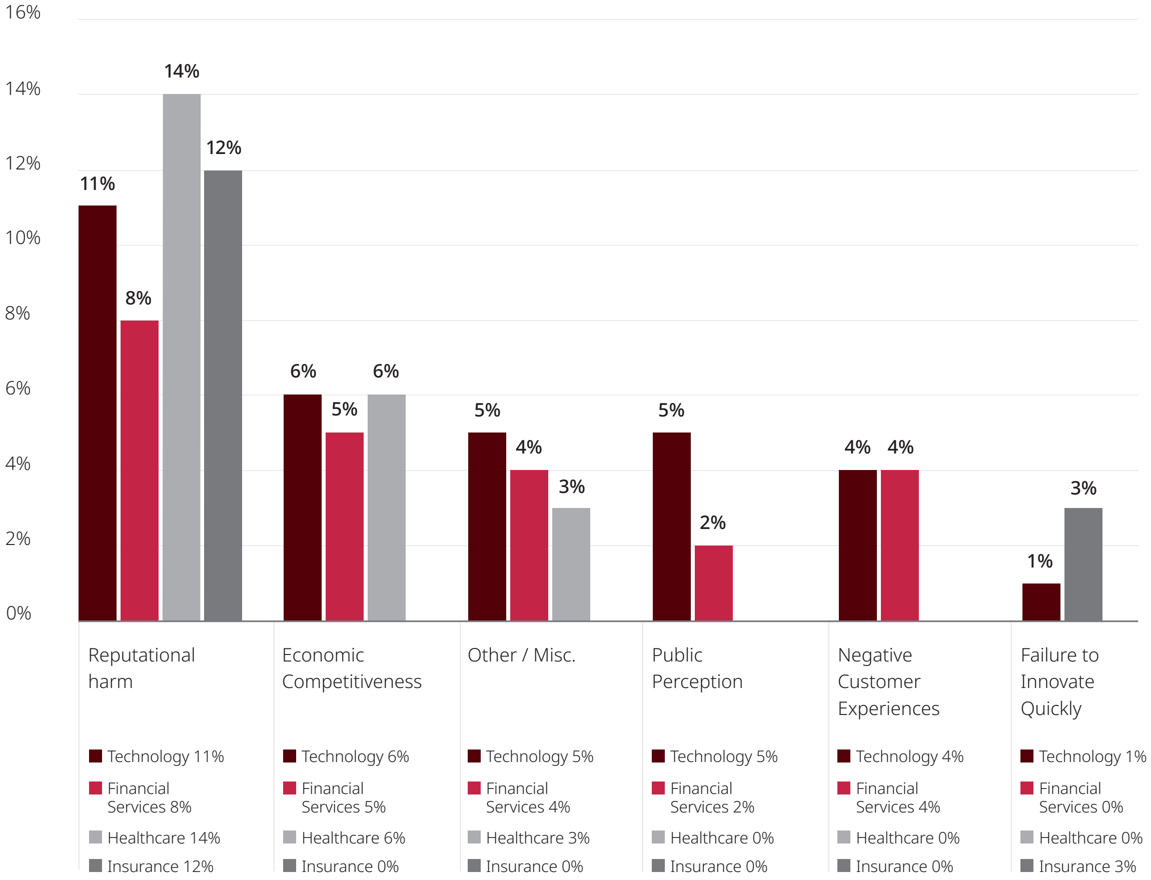
A component of data misuse and consumer protection is fair lending and the risk of deceptive trade practices, which represented 1% of financial services AI risk factor disclosures and 5% of insurance industry AI risk factor disclosures.

Intellectual Property Uncertainty and Infringement Claims (Sector Analysis)



Lack of extensive case law concerning intellectual property protection and artificial intelligence creates uncertainty for companies utilizing AI technology. For example, an AI program may create a solution that resembles another company's product and leave its developers open to IP infringement. Additionally, when an AI system creates a novel invention, there is uncertainty as to the ownership of the invention. A case currently pending before the US Court of Appeals for the Federal Circuit will determine if artificial intelligence can create a patentable invention.

Overall Market Acceptance (Sector Analysis)



Deficiencies and inaccuracies in AI may result in negative customer experience, increasing the risk of negative publicity and reputational damage. Additionally, evolving technologies requires may raise the costs of protecting intellectual property and impacts companies' financial condition and their ability to navigate in a highly competitive market. As AI faces preconceptions and increased regulation, public perception remains a contingency for businesses offering or relying on AI-based solutions. As regulation increases and public perceptions develop, the legal environment for AI may create additional regulatory hurdles.

B. Other disclosures

In addition to Item 105 (risk factors), disclosures related to AI technology may be required under Regulation S-K, Items 101 (business), 103 (legal proceedings) and 303 (MD&A).

A. ITEM 101 (BUSINESS)

Item 101(a) requires a description of the general development of the company's business during the previous five years, or such shorter period as the registrant may have been engaged in business. Under Item 101(a), companies must disclose information material to an understanding of the development of the business, such as material changes to a previously disclosed business strategy.

Item 101(c) requires a more detailed “narrative description of the business done and intended to be done by the registrant and its subsidiaries,” focusing upon the registrant’s dominant segment. Furthermore, any material changes in the mode of conducting the business requires a narrative description of the business done (or intended to be done) by the registrant and its subsidiaries. Disclosures may include the status of development of new products, market and competitive trends and revenue-generating products or services.

A recent DLA Piper Corporate Data Analytics study found that, of the 71 issuers disclosing material AI risks, 28 (or 39%) also specifically referenced AI in their Business section. The vast majority of these companies were in the technology sector, with two issuers in the financial services sector and two in the insurance sector. While some disclosures related to an issuer providing AI-related products and services, most companies discussed AI as a competitive advantage, noting how the company uses AI to enhance their processes and data analysis and/or to provide a better customer experience. According to McKinsey’s 2021 Global Study on AI, which surveyed over 1,000 organizations that have adopted AI, 27% of the respondents used AI for customer service optimization, making this the top most commonly-adopted AI use case.

Common across the Business disclosures was how each company views their usage of AI as a differentiator within their industry, and attribute their market presence and growth to the capabilities that AI provides. Additionally, AI-related business disclosures demonstrate that companies that use AI believe they are able to gather and process more data, optimize operational workflows and obtain efficiencies. A majority of the companies note that their models have improved with the use of AI, allowing them to be more accurate in predicting evolving customer’s needs and creating impact. According to the McKinsey 2021 Global Study on AI, the share of respondents reporting at least 5% of earnings before interest and taxes (EBIT) attributable to AI has increased year over year to 27%, up from 22% in 2020.

B. ITEM 103 (LEGAL PROCEEDINGS)

Item 103 requires companies to disclose any material pending legal proceedings including the name of the court or agency in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis alleged to underlie the proceeding and the relief sought. Similar information is to be included for any such proceedings known to be contemplated by governmental authorities.

Companies have disclosed AI-related legal proceedings disclosures under Item 105 or in the financial statements, but none of the surveyed companies mentioned AI under Item 103.

C. ITEM 303 (MANAGEMENT’S DISCUSSION AND ANALYSIS)

The objective of Item 303 is to “provide material information relevant to an assessment of the financial condition and results of operations of the registrant.” The discussion includes disclosure of known material trends, events and uncertainties.

A recent DLA Piper Corporate Data Analytics study found that, of the 71 companies disclosing material AI risks, 14 (19%) also specifically referenced AI in their MD&A. Of these companies, 11 were in the technology sector, with two in the insurance sector and one in the financial services sector.

Item 303 disclosures are primarily made by companies providing AI-based products or services, and several note the research and development and other expenditures related to AI. According to the McKinsey 2021 Global Study on AI, 22% of respondents use AI to provide AI-based enhancements of products, making this the second most common AI use case. Additionally, product feature optimization (20%), predictive service and intervention (18%), and creation of new AI-based products (17%), are some of the top 10 most common AI use cases.

Conclusion

As the use and influence of AI proliferate, companies can be expected to increasingly need to better understand its benefits and risks to their businesses and stakeholders. These benefits and risks could be significant and potentially disruptive, both to the businesses themselves and within the industries in which they compete. In addition, the regulations and other responsibilities governing the use and impacts of AI are complex, dynamic and varying across jurisdictions.

In this changing environment, we expect to see an increase in the materiality of these topics on businesses and corresponding adaptations to planning, enterprise risk management and control environments. An objective review of the disclosures by public companies to date illustrates a range of potential benefits, impacts and risks, but as AI continues towards its transformative potential, we expect the nature and quantity of relevant disclosures to evolve and grow.

YOUR DESTINATION
50 M

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

For more information

If you would like to discuss the subject of this report further, please contact any of the authors or your DLA Piper relationship partner. Learn more about our firm at dlapiper.com.

John J. Gilluly III
T +1 512 457 7090
john.gilluly@dlapiper.com

Danny Tobey, MD
T +1 214 743 4538
danny.tobey@dlapiper.com

Brooke Goodlett
T +1 512 457 7039
brooke.goodlett@dlapiper.com

This publication is for general information only. The information presented is not legal advice, and your use of it does not create an attorney-client relationship. All legal matters are unique and any prior results described in this publication do not guarantee a similar outcome in future matters. DLA Piper is a global law firm operating through DLA Piper LLP (US) and affiliated entities. For further information, please refer to dlapiper.com. Attorney Advertising. Copyright © 2023 DLA Piper LLP (US). All rights reserved.
Feb 27 2023 | MRS000207222_v6LM