HUNTON
ANDREWS KURTH

FALL 2023

AI and Emerging Technologies

COMMERCIAL CONTRACTING

Generative AI in Contract Terms and Conditions

"The development of full artificial intelligence could spell the end of the human race."

Prof. Stephen Hawking

While it is obviously premature to determine whether Professor Hawking's prognostication will be proven correct, we should not kill off basic elements of contract law along the way. As providers of information technology products and services grapple with how best to incorporate generative AI into their respective products and service offerings, many are realizing that their current terms and conditions do not specifically address generative AI and the risks that are inherent to the technology (or, at least, not currently known). In an effort to allocate liability for the use of (or benefits provided by) generative AI, providers are often ignoring basic tenets of contract law and attempting to unilaterally amend existing agreements with their customers or otherwise strong-arm their way into a more provider-friendly construct.

Depending on the scope of the products and services offered by the provider, adopting such an amendment or agreeing to a provider-friendly approach may significantly increase the customer's exposure to infringement, employment, and privacy-related liabilities, as well as a number of other risks relating specifically to the use of artificial intelligence.

If you have received a communication from any of your providers attempting to amend or otherwise alter the terms of your existing agreement, consider whether you would accept the proffered terms in more typical contexts. We would be happy to assist in reviewing these proposed contract amendments, and have already helped several clients do so.

Jeffrey L. Harvey
Partner, Richmond

PRIVACY AND CYBERSECURITY

Generative AI and US State Privacy Laws: Key Issues to Consider

Companies are rapidly exploring the potential of generative AI solutions, including to automate business processes, improve customer service, generate marketing content and augment communications. While generative AI tools promise a host of benefits to businesses and consumers, there are a number of key issues that organizations must consider under US state privacy laws when developing, onboarding or using generative AI systems.

While the US is still debating AI legislation, comprehensive US state privacy laws include a number of requirements that apply to the use of personal information (PI) in connection with generative AI systems. To date, 13 states have enacted comprehensive privacy laws, with more inevitably to follow in the absence of a federal privacy law. These state laws impose a number of prescriptive requirements regarding notice, individual rights, vendor contracting, processing limitations and internal governance. Key state privacy law issues associated with generative AI include the following:

- The various state privacy laws have codified globally recognized data processing principles, including requirements related to data minimization and purpose limitation. Although these data processing requirements are a foundational backbone to state (and global) privacy laws, they can be antithetical to generative AI technology. For example, compliance with data minimization requirements can be challenging when generative AI systems need copious volumes of data to train and learn. Also, new and unforeseen purposes of generative AI tools can emerge over time as the AI models powering these tools improve and dynamically evolve, leading to tension with the requirement that businesses process PI only for limited and specified purposes.
- In addition to addressing the data processing principles, companies that input PI into generative AI tools, or otherwise process PI in connection with such tools, must ensure that legally sufficient notice has been provided to individuals that their PI may be processed by the system, for what purpose and to whom the PI is disclosed. This can be challenging in the context of generative AI tools that scrape PI from a variety of sources for training, or otherwise where there is no direct interaction with the individual whose PI is processed by the system.

- Companies also need to think about how they effectuate rights requests from individuals. For example, to the extent PI is inputted into an AI system, will it be possible to comply with requests to access, correct or delete the data a generative AI system has ingested?
- Companies also may be required to carry out a data protection impact assessment with respect to their use of generative AI systems, which may be challenging for black box systems that lack interpretability or explainability.
- Further, the majority of companies adopting generative AI solutions are not developing them in-house, which underscores the importance of ensuring appropriate contractual protections are in place for PI made available to AI vendors. In particular, service provider contacts must reflect prescriptive requirements under the state privacy laws. For example, the contract generally must prohibit the service provider from processing PI except on the company's behalf, which

may be difficult if the AI vendor is seeking to use the PI to train its algorithm. To the extent the AI vendor will not agree to a legally-compliant service provider contact, any data sharing with such vendor must be carefully considered to determine whether the disclosure of PI would be considered a "sale" for which individuals have the right to opt out.

- Companies also must consider their data security obligations under the state privacy laws and ensure appropriate technical and administrative safeguards to protect PI processed by generative AI systems. This can be challenging for a number of reasons, including the volume of PI that may be processed by the system, reliance on third parties for AI system development and expertise and the complexity of integrating AI tools with existing systems.

Hunton Andrews Kurth LLP is helping numerous clients navigate compliance with US state privacy laws in the context of generative AI systems, including building AI governance programs and preparing generative AI policies and procedures.

Michael La Marca
Partner, New York

Samuel Grogan
Associate, New York

INSURANCE

Be Smart About Artificial Intelligence: Don't Forget Your Insurance

Artificial Intelligence (AI) is radically reshaping the way business's operate. According to an April 2023 Forbes Survey, among other sources, many business owners are turning to artificial intelligence for activities ranging from increasing productivity, expediting customer service, strengthening cybersecurity, enhancing fraud management, to expanding and enhancing the delivery of healthcare and the development of lifesaving medicines. While the benefits of AI are likely substantial, AI is not without risk. As the use of AI continues to proliferate, the risks and exposures that it presents will continue to emerge. Businesses should be acting now to assess their own unique risks and exposures from the use of AI to ensure that those risks and exposures are appropriately mitigated as part of their existing risk management system.

As previewed in the first installment of the *Hunton Policyholder's Guide to Artificial Intelligence*, AI might, among other things, (1) increase product and service driven liability, particularly where AI-enabled products might generate faulty (or even dangerous) outputs; (2) expose companies to new and additional cybersecurity and data privacy risks; (3) create fiduciary liabilities for directors, officers, and managers who greenlight or fail to oversee AI deployment; (4) result in intellectual property infringement; (5) facilitate unwitting discrimination through algorithmic bias; or (6) compel newly displaced employees to sabotage their former employers. And because the manner and deployment of AI use is rapidly expanding and evolving, and infinitely consequential, one way or another, it should reasonably be expected that most every organization may experience some form of AI-related risk or exposure in the near future.

Of course, businesses effectively manage risk on a daily basis, mainly through insurance but also through other forms of risk transfer. In that way, AI should be viewed like any other peril. Unique to each business, however, is the manner in which it might be affected by that peril. Hence, defining the risk profile should be the first order of business. But to do that effectively, it is necessary to understand how and to what extent the business is utilizing or relying upon AI. To gain this understanding, businesses should consider auditing their unique AI exposures. Indeed, only by first understanding the type of potential AI risks, can businesses best calibrate their insurance and risk transfer programs to mitigate the net financial risk.

Once defined, companies will want to ensure that their insurance portfolio will adequately respond to AI-related liabilities. Today, AI-specific insurance is in its nascency, but at least one

commercial insurer is now offering an AI-specific insurance product. The question remains, however, whether AI risk is new at all, and whether any new insurance product is necessary, or whether existing coverages are sufficiently broad to capture liability that stems from the use or impact of AI. Likewise, companies should evaluate whether existing limits of liability are sufficient to address any enhanced exposure that AI may generate.

In sum, as AI continues to enhance our business capabilities, it is only reasonable to expect it to likewise carry its own unique spectrum of risk and liability. Businesses should be proactive in their assessment of those impacts and be mindful of them when approaching renewal of their insurance and risk transfer portfolios. Stay tuned for future posts from the *Hunton Policyholder's Guide to Artificial Intelligence*, where we will analyze the issues emerging at the intersection of insurance and AI. Our insurance team is at the forefront of this emerging risk and is here to assist clients as they navigate the new and evolving AI landscape.

Michael S. Levine
Partner, Washington, DC

Alex D. Pappas
Associate, Washington, DC

LABOR AND EMPLOYMENT

New York City Regulates Employer Use of Artificial Intelligence

A New York City law regulating the use of so-called "automated employment decision tools" or "AEDTs" took effect this summer. According to guidance issued by the New York City Department of Consumer and Workplace Protection (DCWP) the law applies if the location of the job at issue is, at least part of the time, an office in NYC or the job is fully remote, but the location associated with the job is an office in NYC. The law is a sign of what likely will be a growing trend. New York State legislation governing AEDTs and electronic monitoring tools currently is pending.

The NYC law's definition of an AEDT is longwinded but boils down to a computational process that assigns an observation or generates a prediction to a group and issues a simplified output to substantially assist or replace hiring and promotional decisions by an employer. The law prohibits an employer from using such technology unless: (1) the AEDT has undergone an independent "bias audit" that assesses the tool's impact on ethnicity/race and sex before and within one year of its use; (2) the employer publishes the date of the most recent bias audit, a specific summary of the results, and the date the employer began using the AEDT in a conspicuous manner on the employment section of its public website following each use of the AEDT; and (3) the employer provides a candidate notice identifying information the AEDT uses to assess candidates and instructions to request an alternative selection process or accommodation at least 10 business days before using the AEDT. In addition, an employer must respond to a candidate's written request for the type of data being collected for the AEDT, the source of the data and the employer's AEDT data retention policy within 30 days. Rules enacted by the DCWP further suggest that an employer may need to post this information and instructions for requesting such information on its website. The law provides for monetary penalties that can add up quickly. Violations can be pursued both at the administrative level and in court.

There is no question that a reliable AEDT can save an employer countless money and time spent during the hiring and promotional process. It also can further an employer's bottom line by resulting in the selection of productive employees. In light of the exponential progress we have seen with generative AI in recent days, we very well may see an AEDT that can reliably select the best person for a job in short order. Despite the potential benefit of an AEDT, an employer using or interested in using such technology should proceed with caution. Even if they are not in a jurisdiction that actively regulates such a tool, they soon may be. Moreover, the use of such technology currently can be challenged under numerous federal, state and local employment discrimination laws which outlaw employment processes that have a disparate impact on members of legally protected classes.

Robert T. Quackenboss
Partner, Washington, DC

James J. La Rocca
Counsel, New York

The Growing Influence and Legal Pitfalls of AI in Workforce Management

Artificial Intelligence (AI) is the latest buzzword to permeate the business landscape. Generally, AI refers to computer software that is designed to mimic human decision-making. Companies large and small are rushing to incorporate AI into their business models, particularly in the personnel management space.

Recruitment is the primary sector where businesses deploy AI. These days, almost every employer uses or relies on job search sites that use AI in some way during the hiring process, whether through simple screening tools that weed out applications that don't meet minimum criteria, or more complex recommendation algorithms that rank candidates on likelihood of accepting an offer. Employers also use AI in the performance management context to automate the performance appraisal cycle and generate "continuous" performance evaluation. Thus, employers are able to measure employee productivity in real time, as opposed to once per quarter or year. Employers are also turning to AI for assistance in executing reductions in force. Not only does AI assist employers in making the initial decision to conduct a reduction in force, but it also may help employers decide which employees will be impacted.

Not surprisingly, federal and state lawmakers have noticed the increasing prevalence of AI in the workplace and are taking action. In 2022, the Equal Employment Opportunity Commission (EEOC) issued guidance regarding AI and the Americans with Disabilities Act (ADA), advising employers of their obligation to provide reasonable accommodations to employees who may not be able to interact with AI-assisted hiring software due to a disability. In May 2023, the EEOC issued further guidance, this time regarding AI in the hiring process and cautioning employers against using it in a manner that might create a disparate impact on certain groups of applicants. Critically, the EEOC stated that employers were responsible for the effects of the software they used, regardless of whether a third-party provided or implemented it. Joining the EEOC, the National Labor Relations Board, Federal Trade Commission and Consumer Financial Protection Bureau have all taken steps to adopt standards around or prioritize AI in the coming years.

In addition, states and other jurisdictions have recently begun to enact laws around employers' use of AI. For example, Illinois's Artificial Video Interview Act, passed in 2020 and amended in 2022, requires employers that use AI to analyze video interviews to notify applicants of the practice, obtain affirmative consent to do so and to gather and report race and ethnicity data for applicants who are hired or rejected. The most comprehensive AI regulation is New York City's law regulating "automated employment decision tools" (AEDTs). Among other things, the law requires employers that use AEDTs submit the AEDTs to a bias audit before and within one year of implementation and to publish the date of the most recent bias audit, a summary of the results and the date the employer began using the AEDT in a clear and conspicuous manner on the employment section of the employer's public facing website for at least six months following each use of the AEDT. Washington, DC has put

forth a similar bill, entitled the "Stop Discrimination by Algorithms Act of 2023," which would require employers to have a third party conduct an annual audit of the employer's AI systems and provide a report of the results. In addition, California's Department of Fair Employment and Housing (DFEH) also recently proposed regulations regarding employers' use of AI to screen applicants based on protected characteristics.

The increasing prevalence of AI in the workplace has clearly caught the attention of federal and state regulators. New laws and regulations are sure to come. To prepare, employers should consider reviewing their AI systems and protocols (or the third parties that provide and implement those systems) to understand how those systems make decisions and recommendations. Specifically, employers might consider reviewing what data the system collects, how it collects that data and whether there is a potential conflict with any federal or state regulations. Employers might also consider conducting privileged audits with outside counsel to ensure they understand the legal and statistical nuances of potential disparate impact discrimination and can avoid those pitfalls.

Scott M. Nelson
Partner, Houston

Kevin J. White
Partner, Washington, DC

LITIGATION

Crypto Lawsuits on the Rise—Federal Government Bulks Up Enforcement Efforts and Class Actions Increase

Hundreds of cases regarding emerging technologies have been filed this year, continuing an upward trend from previous years. Many of these cases are being filed in state and federal court in New York, California and Florida, although cases are being seen in jurisdictions nationwide. Topically, cryptocurrency is featured most prominently—accounting for more than three-quarters of emerging technology cases filed in the first half of 2023.

The interest of government regulators and class action plaintiffs in targeting crypto companies has grown as crypto-related scams and frauds have been on the rise. The FTC reports that "[i]n 2022 alone, consumers reported over $1.4 billion in losses to cryptocurrency-related scams."

Several federal agencies have brought suit against cryptocurrency companies and executives this year:

- In *Federal Trade Commission v. Voyager Digital LLC, et al.*, 23-8960 (S.D.N.Y.), the FTC filed suit against Voyager, a company providing crypto-based financial services. The FTC alleged that Voyager deceived consumers, "many of whom were inexperienced with cryptocurrency," into transferring their assets to the Voyager platform. Voyager portrayed itself as a "safe" alternative to the traditional financial system and assured consumers that their funds were insured by the Federal Deposition Insurance Corporation (FDIC). In reality, however, the FTC alleged that Voyager was not FDIC-insured and consumers who held assets with Voyager would not be eligible for FDIC insurance if Voyager failed. In July of 2022, Voyager halted all withdrawals from the platform and subsequently declared bankruptcy—freezing assets on Voyager's platform indefinitely. The FTC announced a settlement with Voyager last month.
- In *Commodity Futures Trading Commission v. Mosaic Exchange Ltd., et al.*, 23-81320 (S.D. Fla.), the CFTC charged Mosaic, a limited liability company, and its owner and CEO for allegedly running a fraudulent digital asset commodity scheme. The CFTC alleged that Mosaic fraudulently solicited and induced at least 17 people in the US and other countries to open accounts and transfer bitcoin for Mosaic to trade. In doing so, Mosaic allegedly falsely represented that it (1) was a cryptocurrency trading platform with tens of millions of dollars under management, (2) had a record of trading profitability, and (3) had partnerships with key cryptocurrency trading exchanges. Despite these representations, many customers of Mosaic ended up losing "most if not all of their money."

- In *Securities and Exchange Commission v. Richard J. Schueler, et al.*, 23-5749 (E.D.N.Y.), the SEC charged Richard Schueler (a.k.a. Richard Heart) and his three unincorporated "alter-ego" entities, Hex, PulseChain and PulseX, with conducting unregistered offerings of crypto asset securities, raising $1 billion from investors. Instead of using the investor money to develop the offerings, the SEC alleged that Schueler misappropriated at least $12 million to purchase luxury goods including sports cars, watches, and a 555-carat black diamond known as "The Enigma."

Several recent class action lawsuits also have targeted crypto companies, including:

- In *Singh v. Illusory Systems Inc., et al.*, 23-183 (D. Del.), plaintiffs Mannu Singh and Iagon AS (a Norwegian corporation) brought suit on behalf of themselves, and others similarly situated against Illusory Systems and other entities behind the Nomad Enterprise—a bridge for transmitting crypto assets from one blockchain to another. Plaintiffs allege that Nomad falsely promised that it employed "state-of-the-art cryptography to protect user assets" but instead "ignored obvious signs that a hack was occurring," allowing $186 million in user assets to be stolen in August 2022.

The increase of government and private scrutiny on crypto assets and exchanges suggests that more crypto-centered lawsuits will follow. For its part, the federal government is directing more resources toward enforcement. In the second half of 2022, the SEC announced that it would add 20 additional positions to its Division of Enforcement's Crypto Assets and Cyber Unit. Said SEC Chair Gary Gensler, "[b]y nearly doubling the size of this key unit, the SEC will be better equipped to police wrongdoing in the crypto markets while continuing to identify disclosure and controls issues with respect to cybersecurity."

Companies delving into the cryptocurrency arena should be aware of this changing legal landscape—both in terms of risk and potential enforcement from government regulators and class action litigation.

Hunton Andrews Kurth regularly monitors new litigation involving emerging technologies and crypto, and the firm has extensive experience in the areas of privacy and cybersecurity, advertising and marketing, class action defense and complex litigation.

Torsten M. Kracht
Partner, Washington, DC

Perie Reiko Koyama
Counsel, Washington, DC

INTELLECTUAL PROPERTY

Copyright Law and Artificial Intelligence

Uncertainty about copyright and artificial intelligence (AI), including fair use of copyrighted works, can arise in the course of your work whether your field is "creative" (e.g., publications, art, or music), "technical" (e.g., software code), or "legal." New law, like the recent Warhol Foundation Supreme Court decision, and emerging technologies, like generative AI and machine learning (ML) models, may leave you with more questions than answers, such as:

- Can the output from an AI generator qualify for copyright protection?
- Does use of copyrighted material in a training set constitute infringement?
- Does the output from an AI generator constitute copyright infringement?
- How can an individual or entity protect anything it generates using AI?

One thing is clear: context matters. A different analysis is required, and potentially a different result may be reached, based on different uses of a given work.

Copyright Law Requires Human Authorship, But What About AI "Prompts"?

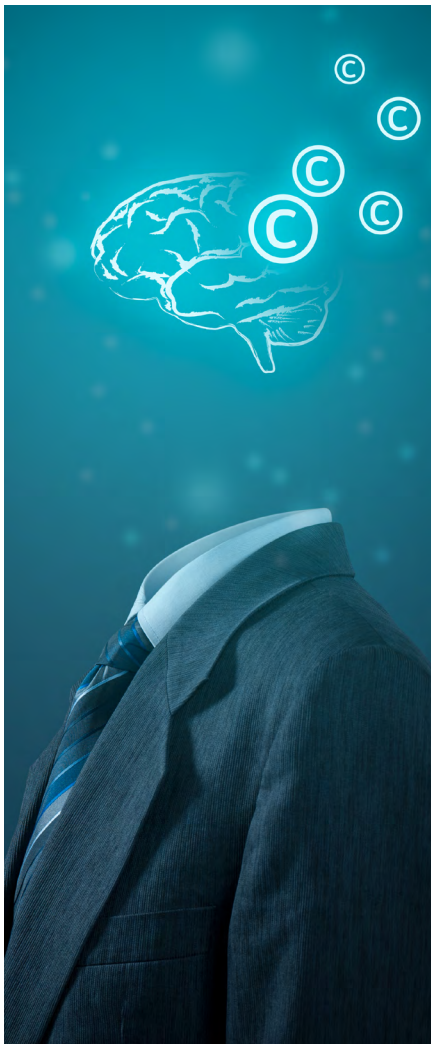
Copyright protection attaches to a work of human authorship fixed in a tangible medium. A machine cannot create a copyrightable work on its own. *Thaler v. Perlmutter, et al.*, No. 22-1564 (BAH) (D. D.C., Aug. 18, 2023).

Thaler is the first district court decision addressing copyrightability of an entirely AI-generated artwork. Hewing to the US Copyright Office's guidance that works entirely generated by AI cannot be copyrighted, the court in *Thaler* upheld the denial of copyright registration. (The court's examination was limited to the administrative record, in which the plaintiff claimed only that he had generated text prompts from which the artwork was then generated by AI.)

Since *Thaler*, the Copyright Office similarly denied registration for a work for which a base image was created by the AI generator Midjourney, which resulted from over 670 successive human-inputted prompts. The Midjourney-generated image was then enhanced in Photoshop by the same human artist who drafted the prompts, adding detail beyond mere color correction.

The Copyright Office intimated that it likely would permit registration of a thin copyright that excluded the AI-generated "raw materials." (This would be consistent with its decision to permit registration of the graphic novel *Zarya of the Dawn* for the entire work and the human-authored text, but not the AI-generated images if used out of context.) However, the artist argued that he should be granted full registration based on his "prompt engineering" in Midjourney and subsequent Photoshop modifications. Because he would not disclaim the AI-generated content, the Office denied registration.

It thus appears that "I created the prompts" will not currently convince the Copyright Office that a work is copyrightable. However, works using AI-generated raw material, but not claiming copyright in that material, will be registrable and treated similarly to a derivative work based on public domain source material: you can protect the resulting whole work and any new human-created elements applied to the work, but cannot enforce rights against an alleged infringer who bases their work on the same AI-generated source material.



Does Copyright Fair Use Apply To AI And Machine Learning?

Fair use is an affirmative defense codified under section 107 of the Copyright Act. It contains four elements and, if found, excuses copyright infringement. As technology pushes the bounds of copyright protection—for example, from copiers to VCRs to online music providers to AI generators—courts continue to wrestle with the definitions and applications of the elements.

A ruling in *Thomson Reuters Enterprise Center GMBH v. Ross Intelligence, Inc.*, No. 1:20-cv-613-SB (D. Del., Sept. 25, 2023), provides a good first-of-its-kind road map of fair use issues presented in ML cases, which may also show how courts will assess fair use in the context of generative AI tools like ChatGPT.

Plaintiff Thomson Reuters (Westlaw) alleged that defendant Ross infringed by copying Westlaw's copyrighted "headnotes" for the purpose of creating a competing legal research platform. Because Ross admitted copying to facilitate machine learning, Westlaw moved for summary judgment. Ross, in turn, defended based on fair use and cross-moved for summary judgment.

The court denied both motions for issues of material fact, but provided an excellent summary of fair use concerns, stressing the first and fourth factors.

The first factor, the purpose and character of the allegedly infringing use, has two parts: commerciality and transformativeness. Quickly concluding that Ross's uses are undoubtedly commercial, the court stressed that commercialism is less significant where the alleged infringing conduct is transformative. The court found that if Ross's version of the facts is correct—*i.e.*, Ross "translated human language into something understandable by a computer as a step in the process of trying to develop a 'wholly new,' albeit competing product—a search tool that would produce highly relevant quotations from judicial opinions in response to natural language questions"—then the final product does not infringe and the use is transformative and favors a finding of fair use.

With respect to the fourth factor, the effect of the alleged infringing use upon the market for the copyrighted work, the court stressed the potential impact of transformativeness, stating: "And transformativeness feeds into this factor as well. '[T]he more the copying is done to achieve a purpose that differs from the purpose of the original, the less likely it is that the copy will serve as a satisfactory substitute for the original.'" Westlaw argued that both parties offer legal research platforms and therefore compete in the same marketplace, but the court expressed skepticism: "One fact is undisputed here: Ross and Thomson Reuters compete in the market for legal research platforms. But that alone does not reveal whether Ross's AI product is a substitute for Westlaw. Ross's use might be transformative, creating a brand-new research platform that serves a different purpose than Westlaw. If so, it is not a market substitute."

The court's comments could apply to any generative AI product. In other words, if the copying necessary to create a generative AI product results in a new, non-infringing product, then such "transformation" not only satisfies the first fair use factor, but also dovetails into the fourth, meaning the new generative AI product has no impact on the relevant market. Specific facts will no doubt matter, but this opinion creates a strong argument that generative AI products qualify for fair use.

John Gary Maynard, III
Partner, Wsahington, DC

Jeremy C. King
Associate, New York

What About Copyright And AI In Other Contexts?

For a more robust discussion of these and related issues, we invite you to view our recent webinar, What's An Acceptable Risk? How Copyright Fair Use Applies To Generative AI: Context Matters.

Additional resources we recommend regarding intellectual property, artificial intelligence, and related policy issues include The USPTO's AI Page, The US Copyright Office's AI Page, and The World Intellectual Property Organization's AI Page.

HUNTON
ANDREWS KURTH