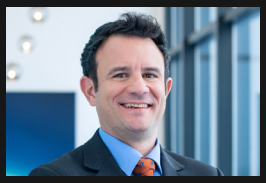
STINSON

AT THE CORNERS

IN THIS ISSUE

CONTACTS



Steve Cosentino, CIPP
PARTNER \ KANSAS CITY
steve.cosentino@stinson.com
816.691.2450

David S. Kim
PARTNER \ ST. LOUIS
david.kim@stinson.com
314.259.4569

Morgan Johnson
PARTNER \ ST. LOUIS
morgan.johnson@stinson.com
314.345.7017

Alli Baden, a 2023 summer associate with Stinson LLP, is currently a law student at the University of Kansas School of Law.

DECENTRALIZED AUTONOMOUS ORGANIZATION LAWS ACROSS THE U.S.

MORGAN JOHNSON

Blockchain technology is a buzzword that has been used by companies for years. In general, blockchain is a decentralized digital ledger used to record and validate transactions. Historically, the focus has primarily been on how blockchain technology may be utilized as a tool to promote businesses; however, the focus has evolved to how blockchain may empower individual users to work toward a common goal in a decentralized manner. In the last few years, blockchain has been used to collate individuals to purchase basketball teams, golf courses, or even bid on a rare copy of the U.S. Constitution.

A collection of individuals using blockchain technologies to work toward a common goal is typically done via a Decentralized Autonomous Organization (DAO). In the simplest example, a DAO takes automated actions using digital "smart" contracts based on the outcome of voting by its members. Voting is typically facilitated through the use of governance tokens residing on a blockchain. Thus, the decisions made by the DAO are open, transparent and decentralized.

DAOs have been used to pool resources of individuals and enter the business world. In 2022, the BIG3 basketball league gave the general public the opportunity to buy a fractional ownership stake in each of its 12 teams in the form of non-fungible tokens (NFT). Two notable DAOs, DeGods and Krause House, purchased the largest controlling stake of their respective teams.

LinksDAO raised $11 million in NFT sales in early 2022, granting each NFT holder a voting right. In February 2023, a reported 80.5% of the NFT holders participated in the vote to acquire the Spey Bay Golf Club in Scotland. The acquisition is now in the formal due diligence phase between LinksDAO and the club.

Despite these recent successful entries of DAOs into the business world, it remains an open question as to how DAOs fit into and will be treated by the current legal framework across the U.S.

Vermont, a first mover in 2018, passed an act related to blockchain business that allowed for the registration of Blockchain-Based Limited Liability Companies (BBLLCs). The state requires that the BBLLC specify the level of decentralization of the company and which participants are entitled to member and management rights in the BBLLC.

The "Wyoming Decentralized Autonomous Organization Supplement Act," passed in 2021, allows for DAOs to register in Wyoming as a DAO LLC and generally operate under the existing LLC laws in the state. This allows for a greater degree of predictability of the treatment of the DAO than in other jurisdictions. As with LLCs, the members of a DAO LLC are generally not personally liable for the debts or obligations of the organization. In Wyoming, if the DAO LLC fails to approve any proposal or take any action for a period of one year, the organization will automatically be dissolved under Wyoming law.

Similarly, a Tennessee act treats registered DAOs as LLCs. Tennessee creates a special decentralized organization status for LLCs that inserts the statutorily-required statement into their articles of organization. These special status LLCs are denoted as either a "DO," "DAO," "DO LLC," or "DAO LLC." The special status entities operate as a normal LLC with respect to personal liability for its members.

The "Utah Decentralized Autonomous Organizations Act," passed in June 2023, takes a much different approach to DAOs. It allows for the creation of a Limited Liability Decentralized Autonomous Organization (LLD). The act requires the certificate of organization, name and address of the individual that is the organizer of the DAO, although the act does provide for a request to redact this information from any public disclosure. The individual members of the DAO are only liable for the on-chain contributions that they commit to the DAO. However, if a judgment or order is entered against the DAO, those that vote against compliance may be liable for monetary payments in proportion to their share of rights in the DAO.

Despite the growing clarity within certain states as to how DAOs are to be treated, most actions of a DAO are "decentralized" and operate almost entirely on the internet. As such, the DAO, its members, or its actions may touch numerous jurisdictions.

For example, a 2022 case brought by the U.S. Commodity Future Trading Commission (CFTC) filed suit against the Ooki DAO, focused in part on the DAO's connections to California. The DAO was alleged to have operated an exchange that allowed for margin (leverage) trading of digital assets. The exchange began as bZeroX, LLC, transferred ownership of the software protocol to bZx DAO, and subsequently renamed bZx DAO to Ooki DAO. According to the CFTC complaint, the founders had believed that transferring ownership to a decentralized organization would insulate the protocol and DAO from compliance with U.S. state and federal laws. The judge determined, under California and federal law, that the DAO was not operating as any specific legal entity, but rather as an unincorporated association of individuals. As such, the judge allowed service of process against the DAO by posting the summons document onto the Ooki DAO online discussion forum and help chat box. Representatives of the Ooki DAO failed to appear before the court and an order granting default judgment was entered June 2023.

Despite the fact that the Ooki DAO case ended in a default judgment, charges were brought against the DAO in a jurisdiction that did not have established DAO LLC or LLD laws. It is clear that several states have made proactive efforts to accommodate DAOs in their legal framework. However, the nature of the internet (and the decentralized manner in which DAOs operate) leaves open the possibility in the foreseeable future that DAOs or their members may be subject to the laws of states that are not favorable to DAO governance or their overall organizational structure.

GENERATIVE AI

DAVID S. KIM

Generative artificial intelligence (AI) programs, like Dall-E and ChatGPT, seem to be all the rage right now. Tech companies big and small are now racing to come up with the next big thing. Like other forms of AI, generative AI analyzes large amounts of data to identify which patterns will be used to create some output. What makes generative AI different is that its output can be used as content, such as text, images, music and videos. In a world where content is king, generative AI has the potential to transform entire industries, including gaming and esports.

Generative AI may be used to create new maps, characters, storylines and even new video games. Such content is generally protected under U.S. copyright law – which is what allows video game developers and publishers to have more control over their games than owners or leagues have in traditional sports. However, AI-created content may not be entitled to any copyright protection, depending on the level of human involvement. For example, after issuing a copyright registration to Kristina Kashtanova for *Zarya of the Dawn*, a graphic novel featuring images generated using Midjourney AI, a text-to-image AI, the U.S. Copyright Office sent a letter on February 21, 2023, regarding their decision to cancel the original registration and issue a new one that specifically excluded content created by Midjourney AI, i.e., the images. The new registration only covered Kashtanova's contributions, which consisted of the text and the selection, coordination and arrangement of the written and visual elements.

The U.S. Copyright Office has long required human authorship for registration and has consistently refused to register works created solely by non-humans. (See §§ 306 and 313.2, Compendium of U.S. Copyright Office Practices (3d ed.)). But, in light of technological advances, is this necessarily the right approach?

In a case before the U.S. District Court for the District of Columbia, Dr. Stephen Thaler, who created Device for the Autonomous Bootstrapping of Unified Sentience, an AI system known to the public as "DABUS,"

sued the U.S. Copyright Office for refusing to register art created by DABUS because it did not satisfy the human authorship requirement. In the U.S., copyright protection exists in an original work of authorship as soon as it is created, with the rights initially vesting in the author. 17 U.S.C. §§ 102 and 201. Typically, that's going to be the person who created the work; however, under current copyright laws, authors need not be human. That's because "works made for hire" aren't authored by their creators, but rather by those who hired their creators, yielding some non-human authors, like corporations and LLCs.

In dueling motions for summary judgment filed earlier this year, Dr. Thaler argued that AI-generated works were copyrightable, and that, as the owner of the AI, he owns the copyright. The U.S. Copyright Office argued that human authorship is necessary to sustain a copyright claim under the Copyright Act and that the Works Made for Hire Doctrine does not apply in this case because DABUS is not a person, employee or agent. The case is still ongoing, and the motions have yet to be decided.

Perhaps a bigger question when it comes to generative AI is in regard to copyright infringement. Copyrighted works may be used to build or train at least some generative AI. While large-scale web scraping of copyrighted material may raise a whole host of legal and ethical issues, from a copyright perspective, there may be good, fair use arguments for using copyrighted material as input for generative AI if its use is transformative and doesn't impact the market for the copyrighted material. See *Authors Guild v. Google, Inc.* 804 F.3d 202 (2d. Cir. 2015).

That said, even if the use of copyrighted material as input may be considered fair use, generative AI could still generate output that constitutes infringement, particularly if that output could be deemed a commercial replacement for the copyrighted work. This is certainly possible where generative AI is already being used to produce works that are "in the style of" specific artists or performers.

Companies that deploy generative AI may have terms of service that purport to limit or prohibit use of copyrighted material, but they could still face secondary liability if they encourage and profit from their users' infringement. See *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005). Moreover, generative AI companies may not be afforded the same protections as other online platforms for its users' actions because generative AI may be seen as an "information content provider" under Section 230 rather than an "interactive computer service."

Still in its infancy, the possibilities of generative AI seem to be endless. The proliferation of generative AI has raised a lot of interesting questions about authorship and copyrights that will likely change the legal landscape for years to come. Companies using generative AI should be proactive about staying on top of the latest developments in both technology and the law.

A NEW TYPE OF FACE PAINTING – THE USE OF FACIAL RECOGNITION TECHNOLOGY IN SPORTS VENUES

STEVE COSENTINO, CIPP AND ALLI BADEN

Professional sports teams' greatest rivals in the coming seasons could be their own fans. With the increase of facial recognition technologies implemented within sports venues, compliance with state biometric privacy laws will be vital in order to avoid hefty fines or class action lawsuits.

Facial recognition technology can be used to collect an individual's biometric identifier. Biometric identifiers are unique physical characteristics, such as a retina scan, fingerprint or a scan of a hand or face geometry, used to identify individuals. Facial recognition captures a person's individual characteristics and maps the geometry of their face. This data is then used to identify the individual. Biometric privacy laws have been put into place to address the sensitive nature of these identifiers. Biometric identifiers such as retina scans, fingerprints and facial scans have an element of permanence that other identifiers and pieces of personal information do not — biometric identifiers cannot be changed if compromised, whereas other identifiers, such as account numbers and numeric identification numbers, can be changed should a breach occur.

The penalties and potential damages associated with biometrics are often more significant than with other types of personal information.

Sports venues around the country have implemented facial recognition into their stadiums to enhance fan experiences. Venues take biometric scans directly from each person and use the scans to expedite what they think is a fans' least favorite part of the game day experience. Venues like Citi Field, home of the New York Mets, and FirstEnergy Stadium, home of the Cleveland Browns, use facial recognition for ticketing. Rather than having to provide a physical a ticket or a mobile pass, patrons stand in front of a camera, the camera scans their face geometry, and their face grants them entry. Venues are expanding this technology to be used at the concession stands as well. A patron's facial scan is connected to their digital wallet, eliminating the need for other payment options. Facial recognition technology can also be used to preserve the moments fans are featured on large venue video displays, including the JumboTron.

Along with enhancing the fan experience, facial recognition can be used for security purposes. Venues can obtain publicly available photos, rather than taking scans from the individual themselves, run a biometric scan on the photo and use the technology to scan the crowd and locate potential threats. States like New York have begun to use biometrics to exclude unwanted or banned individuals from sports venues, including banning adversarial firms and their attorneys from Madison Square Garden.

Though these systems use publicly available photos for scan comparisons, scanning an individual's face and making a match constitutes collection of biometric information in states that have biometric information privacy laws. In this scenario, consent is required and can present some practical challenges, particularly in situations where an individual purchases a ticket and consents to the use of biometrics but then transfers that ticket to another individual. Venues must be careful with how they obtain required consent in order to comply with these new laws. If venues do not obtain proper consent from fans in states that have biometric privacy statutes, they are at risk for fines or lawsuits.

Although there is not a federal biometric privacy statute, Illinois, Texas and Washington have adopted biometric privacy statutes which provide strict requirements for collecting, storing or retaining an individual's biometric data, including information related to facial recognition technology. Generally, a private entity wanting to use an individual's biometric data must obtain the individual's informed consent. If the individual is not provided the opportunity to consent to the use of their biometric information, the private entity is subject to civil or criminal penalties, enforced by the state's attorney general. Further, in Illinois, individuals may bring a private cause of action against the entity for violation of the Illinois statute.

Proper consent to collect and store biometric data varies by state. Although most states have enacted laws that mention biometric collection and storage, they do not require private entities to obtain consent from the individual. Illinois, Texas and Washington all require informed consent before collecting biometric information. Specifically, a sports venue in Illinois must 1) inform the patrons in writing that biometric identifiers or information is being collected or stored; 2) inform the patrons in writing of the purpose and duration for which the biometric identifiers or information will be used; and 3) receive a written release from the patron consenting to the use. Texas also requires informed consent but does not specify the notice and consent must be in writing. New York, on the other hand, requires commercial establishments, including sports venues, to disclose that they are collecting or storing biometric information. The disclosure must be in plain view at the entrances of the establishment, but does not require the establishments to obtain consent for such a use. Residents of New York may also bring a private cause of action if the commercial establishment fails to comply with the statute.

Fans benefit from decreased ticket fraud through the use of biometric identifiers. Both venues and fans benefit from speedier transactions and a more practical method to impose safety policies. As states continue to propose and adopt laws that implicate biometric privacy concerns, sports venues need to be careful about compliance with these laws. Sporting events with sold-out crowds that eventually turn into plaintiffs are not the problems that any teams or venues want to face.

THE LINE UP

01

$2.35 MILLION. In a recent settlement with 17 states attorneys general, undergarment manufacturer Adore Me will pay $2.35 million to resolve claims that it engaged in unfair and deceptive advertising practices. At issue was Adore Me's $39.95 VIP subscription model that charged consumers monthly to gain access to limited and unique pricing discounts. Consumers were required to make a purchase before the sixth day of each month to avoid the monthly charge. Additionally, consumers were automatically opted in to the VIP program without adequate disclosures. Finally, Adore Me used a countdown clock that gave the impression that certain discounts would expire when the clock reached zero The attorneys general claim that it was illegal for Adore Me to lure consumers into a subscription model without adequate disclosures or a reasonable way to cancel. The Adore Me settlement should serve as a warning sign to other businesses that desire to use a subscription model.

02

$50,120. The Federal Trade Commission (FTC) issued new guidance relating to endorsements. Under the new guidance, influencers and endorsers should be expected to provide more "clear and conspicuous" disclosures to the public if they are providing an endorsement. The FTC's guidance is broad and sets forth a subjective standard, which asks whether the audience understands the reviewer's relationship to the company whose products are being recommended. If the audience understands the relationship, a disclosure isn't needed. Noncompliance with the guidance is not legally actionable, but it could result in further investigations by the FTC, including issuance of a notice of a penalty. In the event of a penalty, the FTC could issue fines up to $50,120 *per violation*.

03

$8.5 MILLION. The next round of data analytics has arrived in professional sports. Uplift Labs, a start-up in San Francisco, has been selected by Major League Baseball (MLB) to assist in evaluating the biometrics of future prospects. Using only iPhones and a tripod, the technology can record the biomechanics of an athlete's throwing motion. Utilizing artificial intelligence, this data can be analyzed to determine a scout's potential. It can also assist front offices in evaluating if the prospect may be susceptible to future injury. Currently, over a third of MLB clubs have used the technology. Uplift labs has raised over $8.5 million in a number of capital raises.

04

41. Subject to age requirements, college students may place wagers in jurisdictions that have authorized sports wagering. However, student-athletes are generally prohibited from placing bets and there may be significant eligibility and criminal penalties if they do. In May 2023, 41 student athletes at the University of Iowa and Iowa State University were accused of placing wagers at sports books in the state of Iowa. Those 41 athletes involve prominent sports at both schools, including basketball, baseball and football. The Iowa Division of Criminal Investigation's special enforcement bureau is investigating, which is being overseen by the Iowa Racing Commission. Previously, the National Collegiate Athletic Association (NCAA) stated that "student-athletes who wagered on sports at any level would lose one full season of collegiate eligibility." Under revised NCAA guidelines, the severity of the penalty will vary depending on the cumulative amounts wagered or whether the student-athlete wager on competitions in which they were competing.

05

1,600. As legalized sports wagering continues to expand, betting operators and their users have become targets of criminal conduct. In a recent attack against DraftKings, an American-based daily fantasy sports contest and sports betting company, over 1,600 users had their digital wallets drained in a "credential stuffing attack." According to a criminal complaint, a Wisconsin teenager used the dark web to obtain passwords and usernames that were obtained in prior data breaches. The teenager then used specialized software to hack into a number of user wallets, and was able to siphon over $600,000. When alerted to the fraud, DraftKings took steps to alert users and restore funds to certain accounts.

For more information on these and other esports, sports technology & wagering topics, please subscribe to our quarterly *At the Corners* newsletter.

SUBSCRIBE

LOCATIONS

MINNEAPOLIS
50 South Sixth Street
Suite 2600
Minneapolis, MN 55402
612.335.1500

KANSAS CITY
1201 Walnut Street
Suite 2900
Kansas City, MO 64106
816.842.8600

DALLAS
2200 Ross Avenue
Suite 2900
Dallas, TX 75201
214.560.2201

ST. LOUIS
7700 Forsyth Boulevard
Suite 1100
St. Louis, MO 63105
314.863.0800

PHOENIX
1850 N. Central Avenue
Suite 2200
Phoenix, AZ 85004
602.279.1600

WASHINGTON, DC
1775 Pennsylvania Avenue NW
Suite 800
Washington, DC 20006
202.785.9100

DENVER
1144 Fifteenth Street
Suite 2400
Denver, CO 80202
303.376.8400

OMAHA
1299 Farnam Street
Suite 1500
Omaha, NE 68102
402.342.1700

WICHITA
1625 North Waterfront Parkway
Suite 300
Wichita, KS 67206
316.265.8800

TAMPA
100 Ashley Drive South
Suite 500
Tampa, FL 33602
813.534.7334

NEW YORK
100 Wall Street
Suite 201
New York, NY 10005
646.883.7471

JEFFERSON CITY
230 West McCarty Street
Jefferson City, MO 65101
573.636.6263

BISMARCK
424 South Third Street
Bismarck, ND 58504
701.221.8600

STINSON

STINSON LLP \ STINSON.COM