SHARE:

Join Our Email List

View as Webpage

spilman
thomas & battle

Decoded

Technology Law Insights

Volume 5, Issue 5

Welcome

Welcome to the fifth issue of 2024 of *Decoded* - our technology law insights e-newsletter.

We are pleased to announce that several of the firm's practice groups and attorneys were recognized in the 2024 edition of Chambers USA, a directory of leading law firms and attorneys. Chambers and Partners annually researches the strength and reputation of law firms and individual lawyers across the globe. The research process for the United States includes interviewing lawyers and their clients, including influential general counsel at Fortune 100 companies, high-profile entrepreneurs, and significant purchasers of legal services. Click **here** to learn more.

For those of you interested in the labor and employment law side of issues, we have a recommended conference. We are pleased to announce the return of our in-person *SuperVision Labor & Employment Symposium*, an all-day, free legal seminar being held in Charleston, West Virginia on June 21, 2024. The Symposium will focus on "The Future of Work: Legal Strategies for Employers in a Dynamic Landscape." This program will dive into many hot topics of interest to human resources professionals and anyone who manages employees, including remote work, workplace investigations, artificial intelligence, emerging technologies and privacy, union avoidance, and workplace violence. We hope you can join us for this event. Please click **here** to learn more and register.

Thank you for reading!

Nicholas P. Mooney II, Co-Editor of *Decoded,* Chair of Spilman's Technology Practice Group, and Co-Chair of the Cybersecurity & Data Protection Practice Group

and

Alexander L. Turner, Co-Editor of *Decoded* and Co-Chair of the Cybersecurity & Data Protection Practice Group

FTC Chair: AI Models could Violate Antitrust Laws

"At The Wall Street Journal's 'Future of Everything Festival,' Khan said the FTC is examining ways in which major companies' data scraping could hinder competition or potentially violate people's privacy rights."

Why this is important: There's now another worry to consider when determining how you and your company will use AI. Recently, FTC Chair Lina Khan stated that companies that train their AI models on data from news websites, artists' creations, or people's personal information could be violating antitrust laws. The FTC Act prohibits unfair methods of competition and unfair or deceptive acts or practices. Khan advised that, if a company is using another's content or information in competing with them and diverting business away from them, that practice could be an unfair method of competition. Also, if a company retroactively changes its terms of service to use customers' content in a way that was not disclosed when the content was uploaded, that also could be an unfair method of competition. Khan made clear in her recent statement that government must be involved in determining parameters for the use of AI and can't merely sit on the sidelines. In addition to potential violations of the FTC, which does not have a private right of action for unfair or deceptive acts or practices, companies need to be mindful of the various state acts that are modeled after the FTC Act. Those state acts may permit private rights of action. In those instances, not only must companies be mindful of potential regulation and/or action by the FTC but also must consider the possibility of a civil lawsuit brought by the alleged victim. --- Nicholas P. Mooney II

The Impact of Legacy Vulnerabilities in Today's Cybersecurity Landscape

"Research shows that the vulnerabilities most affecting SMEs are older, known vulnerabilities."

Why this is important: As we all continue to become more interconnected through the "Internet of Things," data privacy and cybersecurity become even more important. While many believe that the latest greatest cybersecurity tools that implement machine learning and AI to detect potential data breaches are the answer, this may not be necessary or accessible for many medium to small businesses as a first line of defense. Many of these medium to small businesses use older hardware and software with unaddressed legacy vulnerabilities. Consequently, the majority of threats medium and small businesses face are not new high tech attacks, but already existing threats that can be more easily, cheaply, and quickly addressed.

Constant vigilance for cybersecurity is a must for any organization. But do not be overwhelmed into inaction by the myriad of possible threats and the perceived cost of protecting your organization. The first step is to have a culture that prioritizes cybersecurity and data privacy at all levels of the organization. Everyone in the organization needs to be invested in protecting the organization's data, and strong leadership in cybersecurity and data privacy from the top is essential for successfully protecting your organization's data. Next steps include installing any neglected software patches to close known software vulnerabilities, and providing data privacy and cybersecurity training for your staff.

Additionally, having annual data security meetings with all department heads, legal counsel, and your organization's IT team is critical. This will allow you to coordinate your organization's approach to cybersecurity and data privacy, and help identify potential weaknesses. During these meetings, you should perform data audits to know what data your organization is holding, what data it needs to keep, and what data should be discarded. More data is not always better, and the more data your organization holds, the greater the risk in the event of a data breach. This team should also be utilized to create and annually update your organization's cybersecurity and data privacy plan, and your data breach response plan. Preparedness now will help save your organization in the future.

While new and emerging technologies to combat bad actors are necessary, do not allow the cost and inexperience with these tools scare you into inaction. Begin with the simple steps first, create your cybersecurity and data privacy team and plans, gain additional knowledge, and move on from there. If you need assistance implementing these steps at your organization, please contact a member of Spilman's Cybersecurity and Data Privacy Practice Group. --- Alexander L. Turner

What Artificial Intelligence Means for the Construction Workplace

"When integrating AI into their business models, construction companies should carefully weigh the costs and benefits of this technology."

Why this is important: Indeed, the construction industry is likely, for the foreseeable future, to continue depending predominantly on human intellect and labor. As the saying goes, "If it isn't broken, don't fix it." However, artificial intelligence (AI) is revolutionizing the construction industry, offering creative solutions to longstanding challenges and innovative methods of workforce expansion. Specifically, two key areas where AI is making a significant impact are improving worker safety and enhancing worker accessibility.

Safety is paramount in the construction industry, where workers face numerous hazards daily. According to Health and Safety Matters, 45 construction workers died in 2022/23, which is a 15 percent increase from the previous year. Historically, workplace health and safety efforts have been enforced and regulated by the Occupational Safety and Health Administration (OSHA), the U.S. Department of Labor agency. Now, in addition to OSHA, AI is increasingly being utilized to mitigate risks and ensure a safer working environment. For instance, AI-powered PPE, such as smart helmets and vests, can monitor vital signs, detect hazardous substances, and alert workers to potential dangers in real-time. Another example is AI-driven computer vision systems which can analyze live video recordings from construction worksites to identify safety hazards/violations, such as unauthorized personnel entering restricted areas or workers not wearing appropriate PPE. However, such safety measures do not only mitigate risks and protect your standard employees. It also opens the door to improving worker accessibility.

Ensuring accessibility for all workers, including those with disabilities or limited mobility, is essential for fostering inclusivity and maximizing workforce potential. Upon enacting the Americans with Disabilities Act (ADA) in 1990, the world's first comprehensive civil rights law for people with disabilities, Congress aimed to expand daily commercial, economic, and social prospects for individuals with disabilities. Under certain circumstances, the ADA mandates that employers offer reasonable accommodations to applicants and employees with disabilities, enabling them to fulfill the essential duties of a job. With the assistance of AI, various solutions now exist to address accessibility challenges for such a physically demanding industry (i.e., the construction workplace). For instance, AI-powered assistive robots can assist workers with physical tasks that may be challenging for individuals with disabilities or injuries. Additionally, AI-driven voice recognition systems can enable hands-free operation of equipment and machinery, allowing workers with mobility impairments to control devices more easily. Altogether, the possibilities seem limitless.

AI has genuine potential to be a powerful resource to improve safety and accessibility in the construction workplace. By harnessing the capabilities of AI technologies, companies within the construction industry can enhance worker health/safety, productivity, and inclusivity, ultimately driving positive outcomes for both workers and employers.

To obtain additional information or guidance concerning what AI means in the construction workplace or how you can appropriately introduce it, reach out to any member of Spilman Thomas & Battle's Construction Practice Group, Cybersecurity & Data Protection Practice Group, or the Labor and Employment Practice Group. --- Malcolm E. Lewis

OpenAI-Scarlett Johansson Voice Flap Continues to Echo

"CEO Sam Altman said the voice wasn't supposed to be 'Her,' but the parallels are many and demonstrate the perils of the super-fast pace of the AI revolution."

Why this is important: OpenAI's recent launch of its chatbot system featured a natural-sounding voice named Sky, which many viewers compared to Scarlett Johansson's AI character in the sci-fi movie "Her." It was later revealed that OpenAI had approached Johansson to use her voice for GPT-4o, but she declined. Researchers then found that Sky's voice strikingly resembles Johansson's, more so than 98 percent of other actors' voices.

National Public Radio (NPR) conducted a study comparing Sky's voice with samples from more than 600 professional actors. The study found that Sky's voice had notable similarities to Johansson's, including specific features influenced by physical characteristics like the throat, mouth, and nasal passages, although there were slight differences in pitch, breathiness, and expressiveness.

OpenAI CEO Sam Altman addressed the controversy, insisting that Sky's voice was not intended to be Johansson's. However, Altman's actions, including a cryptic "Her" post, and the striking similarities suggested otherwise. Johansson was reportedly upset by the resemblance, being protective of her voice and having previously avoided commercial use of it.

Sky has since been removed by OpenAI, but the incident has highlighted the rapid development and potential misuse of voice cloning technology. While it has beneficial applications, such as aiding those who lose their speaking abilities, it also poses risks like voice clone-enhanced phishing. In response to these concerns, the SAG-AFTRA actor's union has updated contracts to specify that only human actors can be credited as voice actors in animated shows and games. --- Shane P. Riley

Ransomware Attacks on Healthcare Impact Nearly Five Times More Sensitive Data

“Twenty percent of a typical healthcare organization’s sensitive data holdings are affected in a ransomware encryption event, compared with an average of just 6% in other industries.”

Why this is important: The U.S. Department of Health and Human Services’ (HHS) Office for Civil Rights has tracked a 256 percent increase in large data breaches involving hacking and a 264 percent jump in ransomware attacks over the past five years. In January 2024, HHS released voluntary cybersecurity goals for healthcare and public health organizations that are broken down into essential and enhanced safeguards, aimed to help organizations prevent cyberattacks, improve their response if an incident occurs, and minimize remaining risk after security measures are applied. At least a portion of HHS’ voluntary goals could become mandatory in the future, with significant penalties for noncompliance, according to the Biden administration’s proposed HHS budget for fiscal year 2025. The ubiquity of cyberattacks means that cybersecurity has become a cost of doing business in healthcare, and it is imperative that healthcare organizations are equipped to prevent and properly respond to cyberattacks. --- Joseph C. Unger

How a CISA Proposal could Impact K-12 Cyber Incident Reporting

“Nonprofit K12 Security Information Exchange has backed the requirement for schools to disclose cyber incidents as generally ‘appropriate.’”

Why this is important: The federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law in March 2022. Among other things, CIRCIA required the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security (DHS) to develop and implement regulations obligating covered entities to report covered cyber incidents and ransomware payments to CISA. In furtherance of this plan, CISA published a notice of proposed rulemaking (NPRM) in the Federal Register in April 2024 to implement CIRCIA.

Adding to the list of federal regulations to which educational institutions are subject, CISA has proposed to include in the description of a covered entity under CIRCIA all local educational agencies, educational service agencies, and state educational agencies, as defined under 20 U.S.C. § 7801, with a student population of 1,000 or more students, as well as institutions of higher education (IHEs) that receive funding under Title IV of the Higher Education Act. The explanation for expanding CIRCIA to cover educational institutions is not surprising. As highlighted by the statistics in this article and the analysis provided by DHS in its 2024 Homeland Security Threat Assessment, schools have been a constant target of ransomware due to budgetary constraints on information technology resources and the likelihood that schools will make ransom payments based on their obligation to function within certain dates and hours. While IHEs are already subject to cybersecurity incident reporting to the U.S. Department of Education under the Gramm-Leach-Bliley Act, that reporting is limited to incidents resulting in unauthorized access to student information. The NPRM expands the scope of reporting required of IHEs to a broader range of cybersecurity incidents and any ransom payments made by IHEs.

In general, the NPRM would require a covered entity to submit a covered cyber incident report to CISA within 72 hours after the entity reasonably believes it occurred. In addition, a covered entity would have to submit a ransom payment report to CISA within 24 hours after disbursement of the payment irrespective of whether the payment is made by the covered entity or a third-party on its behalf. The reporting requirements would apply to a "substantial cyber incident" that leads to substantial loss of confidentiality or network availability or integrity, serious impact on safety and resiliency of operational systems and processes, disruption to business operations, or unauthorized access to information systems or networks or any nonpublic information contained therein caused by specific types of provider or supply chain compromise.

The period for public comment on the NPRM expires on June 3, 2024. CISA expects to publish the Final Rule in 2025. As this article highlights, at least one non-profit leader in the K-12 threat intelligence space is backing the NRPM, but is requesting clarification from CISA on how cyber incidents initiated by students should be reported. As CISA weighs in on public comments and requests for additional information, Spilman attorneys will continue to monitor this impending rule and provide more information regarding its anticipated impact in the education sector. --- Erin Jones Adams

U.S. Senate Releases Roadmap on Artificial Intelligence

"Congress is deliberating a framework for regulating artificial intelligence that would balance responsible enablement with guardrails on civil liberties, copyright, and more."

Why this is important: The U.S. Senate's AI Working Group recently released its roadmap on AI titled "Driving U.S. Innovation in Artificial Intelligence: A Roadmap for Artificial Intelligence Policy in the United States Senate." The roadmap suggests many areas in which AI should be fostered while also being regulated. It suggests that legislation should be passed that implements transparency and disclosure requirements. It also makes clear that the Working Group supports a strong comprehensive federal data privacy law to protect personal information. At the same time, the roadmap suggests many actions that government should take to foster AI-driven innovation in the U.S., such as developing legislation related to training, retraining, and upskilling the private sector workforce to participate in an AI-enabled economy. It also recognizes the uses other countries and governments, like the Chinese Communist Party, are making of AI and suggests that the Senate should consider legislation to combat those uses, like banning the use of AI for social scoring as is done by the CCP and developing a federal framework for autonomous vehicles to compete with the CCP's work in this area. The roadmap covers many areas on which the Senate wants to focus in addressing AI in the near future. It's an easy read, and we recommend that anyone interested in this space review it. --- Nicholas P. Mooney II

Senator Asks FTC, SEC to Investigate UnitedHealth's Cybersecurity Practices

"Sen. Ron Wyden requested that the FTC and SEC chairs investigate UHG's 'numerous cybersecurity and technology failures' to determine whether federal laws were broken.

Why this is important: UnitedHealth Group (UHG) had a significant ransomware attack in February 2024 where bad actors exploited a remote access server that was not protected with multifactor identification. This recent attack was on top of a data breach UHG suffered in October 2022. In addition to $22 million in costs associated with the attack, and the need to shut down the entire data clearinghouse that serves most U.S. medical providers, UHG is now subject to Congressional investigations and increased regulatory scrutiny. Even though the February ransom attack occurred months ago, at a Congressional hearing earlier this month, UHG's CEO still could not identify the extent of the exposure of patient and employee data as a result of the ransom attack. Following that hearing, Senator Ron Wyden (D-Ore.) sent a letter to the Federal Trade Commission and the Securities and Exchange Commission asking them to open investigations into UHG's failure to adequately protect patient and employee data. These requested investigations would be in addition to the Health and Human Services Office for Civil Rights' current investigation into these attacks in relation to UHG's compliance with HIPAA. All of this because UHG failed to take the simple and inexpensive step of putting multifactor authentication on a remote access server. This just goes to prove that cybersecurity and data privacy do not need to be complex and expensive in order to be effective. UHG likely has state-of-the-art cybersecurity in place, but was taken down due to a likely oversight that resulted in a simple tool not being implemented in the correct place. That is why planning and starting with simple solutions first is so important. If your organization needs assistance implementing a comprehensive cybersecurity and data privacy plan, please contact a member of Spilman's Cybersecurity and Data Privacy Practice Group. --- Alexander L. Turner

AI's Role in Heavy Equipment Preventive Maintenance

"AI can be trained to analyze and detect video imagery that would indicate a fault or safety hazard."

Why this is important: As the construction industry technologically advances, so does the integration of Artificial Intelligence (AI) into that technology. An innovative solution to often daunting and complex service operations and customer demands, present in construction operations is AI. With the global AI market projected to reach $621.19 billion in 2024 and soar to $2,740.46 billion by 2032, it's clear that AI's role and influence on the construction industry will be far-reaching and is growing rapidly.

Common challenges in the construction workplace surround issues concerning efficiency and reliability. For improved efficiency, the incorporation of AI may allow contractors to combat low field service productivity resulting from worker downtime, traveling, and administrative tasks. Specifically, AI can allow contractors to automate routine daily tasks (e.g., generating client proposals or planning and scheduling optimization (PSO) software adjusting schedules in real-time), delegate administrative tasks and sales operations (e.g., asset performance review) to AI-driven systems, and ensure efficient travel time by autonomously and digitally generating and routing travel plans. For improved reliability, the incorporation of AI tools like computer vision, which enables machines to "see" and understand their environment, can improve the reliability of operations. In construction industries involving oil and/or gas, such computer vision models can monitor and detect issues such as corrosion, inform users of any necessary maintenance needed, and develop an algorithm to have more routine updates for necessary maintenance.

Further, through AI-driven predictive analytics, equipment performance can be analyzed in real-time and allow for early detection of potential issues before they escalate to costly breakdowns and/or injuries. What is more, and ancillary to such positive outcomes, the continued integration of AI-driven systems into construction safety operations will afford heavy equipment operators the ability to ensure optimal performance, reduce operational costs, and extend the lifespan of their machinery.

Overall, the benefits and capabilities of incorporating AI into the construction workplace appear infinite. It is no secret, that AI represents a paradigm shift in the construction industry, offering unprecedented capabilities to enhance productivity, reliability, and efficiency. As the construction industry continues to adopt and adapt to these technological advancements, it will undoubtedly reap the benefits of such capabilities.

To obtain additional information, guidance, and/or to evaluate your existing AI efforts in your current construction operations, it is encouraged that you reach out to the authors of this publication or any member of Spilman Thomas & Battle's Cybersecurity & Data Protection Practice Group or Construction Practice Group. --- Malcolm E. Lewis

New Modified CRISPR Protein can Fit Inside Virus Used for Gene Therapy

"Recent years have seen an explosion of research attempting to harness CRISPR gene-editing systems—which are found naturally in many bacteria as a defense against viruses—so they can be used as potential treatments for human disease."

Why this is important: Researchers from Wuhan University, China, led by Hongjian Wang, have developed a new, smaller version of the CRISPR gene-editing protein Cas12a, called enEbCas12a, which shows high editing efficiency. This modified protein, derived from a natural Cas12a variant found in Erysipelotrichia bacteria, can be packaged within a non-pathogenic adeno-associated virus (AAV). This is significant because AAVs are often too small to carry larger Cas12a proteins.

In lab tests, enEbCas12a demonstrated gene-editing efficiency comparable to other accurate Cas12a proteins. The research team successfully used AAVs to deliver enEbCas12a to target a cholesterol-related gene in mice, resulting in significant reductions in blood cholesterol levels after one month.

The study suggests that enEbCas12a could potentially be used for human gene therapy, providing a compact and efficient tool for gene editing. Further research is required to confirm its efficacy and safety in clinical applications. The findings indicate that this approach could facilitate advanced gene-editing therapies, including multi-gene, base, and prime editing, delivered via AAV systems. --- Shane P. Riley

Norfolk Southern and CSX Sue Cox Communications Over Broadband Installations

"The lawsuit responds to Cox's use of a new state law that legislators said will streamline the process for getting internet access across railroad crossings to rural users."

Why this is important: As an attorney who regularly works with public entities who have contracts with other public entities with contractual requirements to build out broadband service to underserved areas that are seeking to cross portions of Virginia's extensive railroad network, I can sympathize with how time consuming and expensive it is to cross rail lines. I also work with public entities trying to cross rail lines for all sorts of utilities, from water to broadband. But the railroads are right that in all other circumstances I am aware of in which someone has a right to cross railroad tracks over a railroad's objection or tries to override the railroad's demands, the railroad is paid just compensation as determined by a court. There is even a specific statute, Virginia Code § 25.1-102, that allows the State Corporation Commission to mediate these types of disputes. But under the circumstances where there is vast federal money at issue that must be returned if it is not spent by a hard statutory deadline, these types of delays can easily kill internet access in areas of the state. An interesting wrinkle here, however, is the new Net Neutrality ruling by the FCC. The FCC recently reclassified broadband providers as telecommunications providers under Title II of the Communications Act of 1934. While internet companies have understandably focused on how this affects their ability to sell bandwidth, one of the positive side effects may be that broadband providers could qualify for certification by the SCC as "telecommunications" providers who have the right of eminent domain. As usual with new statutes, new declaratory rulings, and federal litigation, it will be an interesting ride worth keeping track of for those with an interest in utilities law. --- Michael W.S. Lockaby

Test AI Now, but Know the Risks, Panelists Say

"Speakers at the annual NIBS conference recommended using the 'gorilla test' and other techniques to monitor the technology as it evolves."

Why this is important: At the recent National Institute of Building Sciences Building Innovation Conference, in Washington, D.C., industry experts encouraged exploration into the generative AI space. Many of the advantages of artificial intelligence are known; however, the results across software platforms are not homogenous. During live examples, panelists at the conference demonstrated the flaws of various generative AI models, via a test of two models to find the instances of the word "gorilla" in a spreadsheet of miscellaneous data. There was a 50 percent accuracy rate.

AI models are not perfect, hallucinations -- instances where the technology makes a mistake or invents arbitrary responses -- happen frequently enough for general warning against blind reliance. Nevertheless, the advantage of incorporating AI into the construction sector is predominantly in workflow. The capacity of AI to filter through copious reports and manuals and expeditiously articulate a response can significantly accelerate the pace of project management with a reasonable sense of confidence. AI should not replace oversight and general professional compliance standards. However, advanced technology will creep into every industry whether leaders are opposed or not; the only question leaders need to consider at this point is how prepared they are to stay at the cutting edge of what is already possible. --- Sophia L. Hines

4 Ways GenAI in Healthcare Improves Patient Experiences

"The healthcare industry has proven to be the perfect playground for the introduction of GenAI, or generative artificial intelligence, and has the potential to significantly improve patient CX journeys via contact centers and hospitals."

Why this is important: Developments in GenAI, or generative artificial intelligence, are profoundly impacting our everyday lives, and unlocking new opportunities for growth and innovation at lightning speed. By viewing this rapidly evolving technology through the lens of customer service, we can begin to appreciate the positive impact that artificial intelligence is making on patient outcomes in the healthcare industry. The "CX journey," or, "customer experience," contemplates every interaction between a business and customers, from start to finish. In the context of healthcare, this includes everything from the first phone call to schedule an appointment, to the time spent in a waiting room, to the quality of care received. Advancements in the following areas have been highlighted:

- Boosting efficiency in the contact center. Issues such as test results, or scheduling an appointment, can be fielded by GenAI, reducing lengthy call times and patient stress.
- Enhancing data personalization. GenAI can tailor specific patient recommendations, identify earlier interventions and preventive measures, and significantly reduce business costs.
- Expanding telehealth processes. By diagnosing common ailments and providing treatment recommendations for home, GenAI can reduce the risk of unnecessary patient exposure.
- Reducing administrative burden and improving workflows in hospitals. Providers can use GenAI to create clinical notes in real-time with hands-free devices, allowing increased focus on patient care.

Key takeaway: These developments are making a real impact on patient outcomes, and, a strong command of emerging GenAI technology will certainly become a necessary component of litigation arising from patient care. --- Ralph "Joe" J. Hagy

Share This Email Share This Email Share This Email

This is an attorney advertisement. Your receipt and/or use of this material does not constitute or create an attorney-client relationship between you and Spilman Thomas & Battle, PLLC or any attorney associated with the firm. This e-mail publication is distributed with the understanding that the author, publisher and distributor are not rendering legal or other professional advice on specific facts or matters and, accordingly, assume no liability whatsoever in connection with its use.

Responsible Attorney: Michael J. Basile, 800-967-8251

Spilman Thomas & Battle | 300 Kanawha Blvd., E. | Charleston, WV 25301 US