SHARE:

Join Our Email List

View as Webpage

November 10, 2022

Welcome

Welcome to the 22nd issue of *Decoded* for the year.

We are extremely pleased to announce that Spilman was named to the 2023 "Best Law Firms" list by *U.S. News-Best Lawyers* in 61 areas of law throughout the firm's footprint - including several areas dealing with technology.

The rankings are based on a rigorous assessment process that involved the collection of client and lawyer evaluations, peer review from leading attorneys, and review of additional information provided by law firms. You can learn more here.

We would also like to introduce you to one of our new colleagues in Spilman's Pittsburgh office: Shane P. Riley. His primary areas of practice are corporate law, patent law and intellectual property law. Shane assists clients in the areas of technology and data privacy law. He has extensive experience advising on data privacy issues, including compliance with HIPAA/HITECH, FERPA, GDPR, CCPA, and CPRA, along with other institutional concerns, such as confidentiality, export control, risk management, and conflict of interest. Shane also has extensive experience advising clients on intellectual property ownership, protection, and licensing issues across a broad range of disciplines. He drafts and negotiates various corporate and research related agreements, clinical trial agreements, confidentiality and nondisclosure agreements, material transfer/use agreements, and collaboration agreements. He also guides researchers and inventors through the legal processes and best practices necessary to protect the integrity of their work. Prior to joining Spilman, he served as Assistant Director for Clinical/Corporate Contracts at the

University of Pittsburgh. He earned his undergraduate degree in biological sciences and his law degree from the University of Pittsburgh as well.

We hope you enjoy this issue and, as always, 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

---

The Supreme Court has Made It Harder to Regulate New Technologies

"However, the way the Supreme Court did this—by recognizing and endorsing the 'major questions doctrine'—threatens regulation and public policy in the U.S. by allowing judges to pick and choose regulation they think is 'major' and then undoing it."

Why this is important: The Supreme Court is shifting its stance on the regulation of new technologies by recognizing the "major questions doctrine" and giving less deference to the agencies authorized by Congress to speak to certain issues within their general scope. Federal agencies are empowered to interpret the statutes that grant them authority when forming regulations around new technology, and the Court has historically sided with the agencies' interpretations of the law when it is ambiguous. The "major questions doctrine" embraces the Court's ability to challenge an agency's claims of regulatory authority when the issue at hand has broad economic and political significance, essentially overriding their authority and choosing for themselves what is in and out of bounds under an ambiguous Act of Congress.

This article does well to point out that new technology almost always has vast economic and political consequences. Since unforeseeable concerns are inherent in new technology and the authority granted by Congress does not often speak specifically to them, the embrace of the "major questions doctrine" heartily increases the Court's influence and power in policymaking. This injects new uncertainty and political considerations moving forward for businesses at the cutting edge of tech. It is difficult to predict when and how the Court will intervene, and what, ultimately, will be considered "too political" to allow the authorized agency to regulate.

This may be a part of a new trend by the Supreme Court to be more involved in the policymaking around highly technical innovations. The Court also has recently agreed to hear an appeal by Amgen, Inc. regarding their efforts to block competitor drugs they claim infringe on their patents despite a rejection of the suit by the Court of Appeals and the Justice Department's recommendation not to hear the case. In their review, the justices will consider whether Amgen can benefit from older broad claims that new innovators argue will hinder valuable incremental progress in various fields that are quickly advancing. While the direction the justices take is yet to be seen, it is clear that technology firms of all sizes should be paying attention to the Court's undaunted approach to high tech moving forward. --- Shane P. Riley

---

Experts Remain Divided on N.C. Ransomware Payment Ban

"Nearly a year after the state passed a law making it illegal to pay cyber criminals to regain access to encrypted systems, not everyone is convinced the ban is going to put a dent in the number of cyber attacks in the state."

Why this is important: In a recent edition of *Decoded*, we discussed the ransomware attack on the Los Angeles Unified School District ("LAUSD"). In response to that attack, the LAUSD reached out to the White House for assistance on how to respond. The Biden administration responded with instructions not to pay the ransom, which the LAUSD followed. If this same attack had occurred in North Carolina after April 5, 2022, the school district would not have a choice on how to respond to a ransomware attack. As part of North Carolina's 2021-2022 budget appropriation, the new law prohibits government entities from paying a ransom to a ransomware attacker. In fact, the law prohibits the government entity from even communicating with the attacker. Instead, all ransomware attacks are to be reported to the North Carolina Department of Information Technology. This law applies to all governmental entities, including local governments, public schools and the University of North Carolina system. While the new law does not apply to private entities, they are still encouraged to report cyber attacks to the Department of Information Technology. The North Carolina law is the first of its kind in the country. Pennsylvania subsequently passed a similar law, and New York is considering passing a analogous law.

The question now is how is the new law working out in preventing ransomware attacks against governmental entities in North Carolina. In the first half of the year, two cities, two school districts, three colleges and one state agency in North Carolina experienced ransomware attacks. The State of North Carolina says that the new law has been successful in lowering cybersecurity incidents from 2021. Cybersecurity experts are more skeptical as to the effectiveness of the new law, and need more time to evaluate its ability to deter ransomware attacks. One issue is that prohibiting payment of a ransom may not deter attackers because they do not necessarily act rationally. Some cybersecurity professionals believe that it is better to promote cybersecurity training and funding, which the new law does not do. Overall, the effectiveness of the new law will have to be judged over a longer period of time. --- Alexander L. Turner

---

FTC Takes Action Against Online Education Service Chegg for Data Breaches and Student Information Exposure

"This data as well as other personally identifying information belonging to users and employees was leaked in a series of breaches, including two phishing attacks, and the infiltration by a former contractor of Chegg's Amazon Web Services database."

Why this is important: The FTC recently took an enforcement action against Chegg, Inc. ("Chegg"). Chegg markets and sells direct-to-student educational products and services. Pursuant to Section 5 of the FTC Act, the FTC has the ability to bring enforcement actions against companies for unfair and deceptive trade practices. In relation to cyberattacks, for the past few years, the FTC has been focused on unfair practices by companies that result in a data breach. These unfair practices include when a company fails to implement adequate protective measures for sensitive personal information.

The enforcement action against Chegg was related to four data breaches Chegg experienced between 2017 and 2020. These data breaches were significant because Chegg collects sensitive data on its high school and college student customers. This data includes information regarding religious affiliation, heritage, date of birth, parents' income range, sexual orientation, and disabilities. These attacks included two phishing attacks and an infiltration by a former contractor. The attacks were successful because, as alleged by the FTC, Chegg engaged in an unfair practice when it failed to implement basic security measures to protect students' sensitive information. This included the fact that Chegg failed to require employees and contractors to use multifactor authentication to login to databases, failed to monitor networks and databases for threats, did not properly encrypt personal data and passwords, and did not

maintain adequate security policies and training. The result was 40 million Chegg customers had their data stolen. In a resolution of the FTC enforcement action, Chegg agreed to limit data collection, use stronger protections, and implement a training and compliance program. While Chegg was not required to pay any penalties, it was required to notify customers on how to protect their identities. Chegg got lucky and was not assessed a financial penalty by the FTC, but the requirement that it notify its affected customers may result in costly civil litigation. --- Alexander L. Turner

---

Lawsuit Alleging Amazon's Alexa Is Spying on You Moves Forward and TikTok's Class Action Settlement Sparks Greater Privacy Concerns

"Amazon lost a round in a court when a federal judge ordered the internet retail giant to produce millions of documents in a legal battle over the marketing of its Alexa-enabled devices and their recording of users' conversations."

"However, the company's privacy policy reveals how the app takes its data collection several steps further than most others on the market."

Why this is important: Do you even know how much privacy you surrender each day - voluntarily! – to internet service platforms? Please read these articles for insight. Amazon Alexa is a wonderful tool. Especially older people, who are not comfortable on a computer, find it helpful. It also captures and analyzes much of what it "hears" in the environments where it is located. TikTok is not, as some have alleged, "Chinese spyware," to the best of my knowledge. But its license does provide broad access to almost everything important on the user's computer, including the files! These are just two of many such apps. All of this is described (in highly technical terms) in the license for whatever app is guilty of this behavior. As a people ("sheeple?"), we ignore these risks to our privacy in order to save a little time or enjoy the next hit of dopamine. There is a reason that when you review a recipe online, you suddenly get ads for fancy flour and spices. There is a reason that when you tell your spouse or child that you are looking at trading-in the old minivan, you get ads for SUVs. And, there is a reason that when you send an email to your sister promoting a political candidate, you receive articles recommending the other candidate. If you have nothing personal on your computer, okay. If this sharing of privacy does not give you pause, fine. If you do have private information on your computer that you do not want to share, you must lock it away (see your IT), place it in files that are encrypted, and take other protective steps. OR, even better, you must make the painful decision to eliminate from your household or business all purveyors of this assault on privacy. --- Hugh B. Wellons

---

Pennsylvania Settlements with Experian and T-Mobile

Why this is important: Pennsylvania's Attorney General, Josh Shapiro, announced on Monday, November 7, 2022, that Pennsylvania entered into settlements (Experian #1, Experian #2, and T-Mobile) with Experian and T-Mobile related to data breach incidents that Experian experienced in 2012, and that both companies experienced in 2015. This agreement between the parties resolved a multistate action by a number state Attorneys General. The total monetary amount for the settlements was $16 million, of which the State of Pennsylvania is entitled to $464,000. The settlements also included requirements that the companies strengthen their data security practices.

Experian's 2012 data breach involved an Experian subsidiary, Experian Data Corp. ("EDC"). That data breach involved an identity thief who posed as a private investigator in order to gain access to

consumers' personally identifiable information ("PII"). In addition to a monetary settlement, Experian is required to:

- Strengthen its vetting and oversight of third parties requesting access to consumers' PII;
- Investigate and report data security incidents to the Attorneys General; and
- Maintain a "Red Flags" program to detect and respond to potential identity theft events.

This action settled for a $1 million of the total $16 million settlement.

The larger settlements involved a 2015 data breach where an unauthorized actor gained access to the part of Experian's network that stored the personal data on behalf of its client, T-Mobile. This data breach included consumer information related to applications for T-Mobile's postpaid services and device financing between September 2013 and September 2015. The information obtained by the unauthorized users included consumer PII and T-Mobile's internal credit assessments. In total, 484,147 Pennsylvanians were impacted by this data breach.

In addition to obtaining a monetary settlement from Experian and T-Mobile, the settlements also included requirements that the two companies strengthen their data security practices. For Experian, this included:

- Prohibition against misrepresentations to its clients regarding the extent to which Experian protects the privacy and security of personal information;
- Implementation of a comprehensive Information Security Program, incorporating zero-trust principles, regular executive-level reporting, and enhanced employee training;
- Due diligence provisions requiring the company to properly vet acquisitions and evaluate data security concerns prior to integration;
- Data minimization and disposal requirements, including specific efforts aimed at reducing use of Social Security numbers as identifiers; and
- Specific security requirements, including with respect to encryption, segmentation, patch management, intrusion detection, firewalls, access controls, logging and monitoring, penetration testing, and risk assessments.

The settlement also requires Experian to offer five years of free credit monitoring services to affected consumers, as well as two free copies of their credit reports annually during that time frame. As part of this settlement, T-Mobile was required to:

- Implementation of a Vendor Risk Management Program;
- Maintenance of a T-Mobile vendor contract inventory, including vendor risk ratings based on the nature and type of information that the vendor receives or maintains;
- Imposition of contractual data security requirements on T-Mobile's vendors and sub-vendors, including related to segmentation, passwords, encryption keys, and patching;
- Establishment of vendor assessment and monitoring mechanisms; and
- Appropriate action in response to vendor non-compliance, up to contract termination.

This settlement with T-Mobile does not include a separate data breach that T-Mobile suffered in 2021. That incident is subject to a separate investigation. --- Alexander L. Turner

---

Pennsylvania's Newest Autonomous Vehicle Legislation is Poised to become Law. Here's Why It Matters.

"The public is still erring on the side of caution on the topic of AVs, with a Pew Research Center poll conducted in 2022 showing that 44% of Americans feel driverless cars are a 'bad idea.'"

Why this is important: On November 3, 2022, Governor Wolf approved Act 130 of 2022 (HB 2398-Bill). Proponents of the legislation note that it will modernize the Commonwealth's vehicle code pertaining to autonomous vehicles. This legislation would allow for the driverless testing and deployment of autonomous vehicles in Pennsylvania. It would allow platooning with a driver in the lead vehicle and one nonlead vehicle would be allowed to operate with an automated driving system subject to the plan's review by the Pennsylvania Department of Transportation. Some members expressed concerns that the legislation would have a negative impact on Pennsylvania's workforce. Those who supported the measure replied to such concerns by highlighting the need for Pennsylvania to remain competitive in this technology sector and the potential for increased revenues and jobs. Governor Wolf also commented on the concerns by noting that he encourages the Pennsylvania General Assembly to ensure that workers are protected and permitted the opportunity to participate as the industry grows.

As noted above, many citizens are cautious when embracing this new technology and this is reflected in the number of members who voted against the legislation. Proponents of the legislation would likely respond that it is wise to embrace the technological advancements and create a regulatory framework to ensure the public's safety. --- Annmarie Kaiser Robey

---

How Cybersecurity Experts are Reacting to CISA's New Security Goals for Critical Infrastructure

"Federal authorities describe the cross-sector guidance as 'a floor, not a ceiling.'"

Why this is important: The new security goals for critical infrastructure is about crawling before you walk before you run. The Cybersecurity Infrastructure Security Agency recently released security guidelines for critical infrastructure. The guidelines are voluntary, and they are basic. The guidelines reflect the fact that a majority of U.S. critical infrastructure is owned and operated by private companies. Those companies have implemented security protocols in varying degrees, and the CISA found that many do not have protocols that cover even the most basic security concepts, like multi-factor authentication, strong password management, and maintaining backups. CISA hopes the guidelines will get all critical infrastructure companies on the same page about basic cybersecurity protocols, foster a mindset that we're all in this together, and provide a starting point for implementing more robust protocols. --- Nicholas P. Mooney II

Mandate Issues in AI-Developed Technology Patent Dispute After Fed Cir. Denies Rehearing

"Thaler argued that his AI system, 'Device for the Autonomous Bootstrapping of Case Unified Science,' or 'DABUS,' a collection of source code and a software program, was the inventor of two patents, but the PTO disagreed, finding the patent applications as incomplete because they did not list a human as the inventor."

Why this is important: Stephen Thaler's attempts to obtain patents he claims were invented by his AI system exhibit a growing area of debate among innovators and patent practitioners alike. Presently, only human beings may be considered inventors for the purpose of obtaining a patent; a fact bolstered by the Federal Circuit's recent ruling against Thaler. To be considered an inventor, an individual must contribute to the conception of the subject invention by having formed in their mind a complete idea of the operative invention with enough specificity that they would be able to explain to someone skilled in the

art how to make or use the invention. Claiming inventorship by AI steps outside this traditional view of the process of invention, which is fixed to the human mind. Up until now, AI has only been considered a tool used by inventors, not an inventor itself. A major question is whether an individual can claim they invented something when an AI system precluded them from meaningfully contributing to its conception. If they cannot and non-humans are not able to be inventors under patent law, then whole classes of new innovations developed through AI could be deemed unpatentable and, thus, become highly guarded from the public at large. After issue of the Court of Appeals' recent mandate, Thaler may decide to appeal to the Supreme Court, which, if heard, would bring the issue and the debate to center stage. --- Shane P. Riley

---

Biotechnology is Creating Ethical Worries—and We've been Here Before

"Over the past decade or so, as CRISPR was discovered and applied to genetic remodeling, he started to get concerned—afraid, actually—about three potential applications of the technology."

Why this is important: I know, I've beaten this drum before. Biotech ethics is a passion of mine. (I even helped pen a chapter about it in *Biotechnology and the Law*, published by the American Bar Association.) CRISPR and later gene-altering technology provide promise, but also danger. The 2020 Nobel Laureate, and one of the inventors of CRISPR, recently wrote *As Gods: A Moral History of the Genetic Age*, a book describing the major fears that the author has about this developing technology. This article reviews the book and provides short summaries of three uses of genetic engineering that may pose the most danger. They are: 1. **Introducing mutations into the human genome** that can be inherited (and spread); 2. **Gene drives**, that allow a mutation to copy itself from one chromosome to another, almost ensuring the survival of that mutation; and 3. **Gain of function ("GOF") research**, meant to expand possible pathogens to study the likelihood of human infection and, ostensibly, to develop vaccines and treatments, in case such pathogen should develop or escape. We do not know specifically where COVID-19 came from, but the current nexis seems to be Wuhan, China, where a large lab studied similar viruses, and some GOF research was occurring. Even if the lab was not the cause this time, these are not future dangers, they are here, already. --- Hugh B. Wellons

---

Collecting Personal Data Improves Safety, but Increases Contractor Liability

"As more contractors adopt safety technology that collects and stores personal data, including CCTV monitoring, GPS location tracking and weight sensors on drivers' seats, maintaining privacy and protecting sensitive information about workers—who are concerned that their personal data could be misused, sold to third-party vendors or stolen by hackers—has become a crucial responsibility."

Why this is important: Worker safety on the jobsite is always a priority on every construction project. To establish the safest possible working environments, construction companies have turned to technology to monitor their workforces and workplace safety. This technology includes a system in which the worker signs in each morning and answers a simple question: Why do you want to be safe today? Answers are generally thoughtful, and sometimes include uploads of pictures of workers' families. The goal is to get the workers to have safety in the forefront of their minds and to remind them about why safety is so important. Other safety technology includes wearables, sensors, CCTV monitoring, AI tools and extended-reality platforms.

This personal data that construction companies collect from their employees through these technologies in an attempt to promote a safe work environment is valuable and must be protected. Concerns regarding data theft and sale are warranted because the construction industry is a big target of ransomware. That is because the construction industry has traditionally been lax in protecting its data. Additionally, workers also have reason to be concerned about the sale of their personal data that is collected through these new safety technologies because a lot of the vendors that are providing these products are selling the data they are collecting to third party advertisers.

Wearables and other safety devices that collect biometric data also open up construction companies to liability. Workers are concerned about how that data may be used, and if that data can be used against them in the future. States like Illinois have strict laws regarding the collection of biometric data. The Illinois Biometric Information Privacy Act ("BIPA") requires employers who collect employees' biometric data to follow a number of protocols. These protocols include (1) maintaining a written policy about the collection and storage of employee biometric data, (2) providing employees with written notice of the data collection and storage policy, and (3) obtaining informed consent from employees to collect biometric data. Biometric data goes beyond safety-related technology, and extends to fingerprint and retina readers for time systems and building access, as well as face recognition systems.

Safety is paramount on every construction project, but so is data security. If your company is going to use safety technologies to monitor employees, be sure that you adequately secure the data that those technologies generate; that you review your contracts with safety technology vendors to ensure that your employees' data is not being sold; and that you abide by state and federal laws regarding protocols for data security, biometric information collection, and data breach notification and response. If you would like assistance in formulating a data security and data breach plan, or have questions regarding implementing safety technologies on your next project, please contact Spilman's Data Privacy and Cyber Security Practice Group. --- Alexander L. Turner

---

The Future of Developing Innovative Designs Based on DNA Nanotechnology

"Electronic and photonic devices have unique functionalities for converting chemical and biological processes into electrical or optical signals to detect, identify, and monitor these processes."

Why this is important: DNA nanotechnology is demonstrating expanded applications and has the potential to be a highly useful and efficient innovative tool in cutting edge fields, but lacks the broad commercialization effort that could deliver the technology to consumers. As innovation gets physically smaller, programming DNA to assemble nanostructures appears to become more and more advantageous and achievable. This article details the study of four potential applications: quantum computing, carbon nanotube transistors, enzymatic fuel cells, and artificial electromagnetic materials. In all cases, the application of DNA nanotechnology provided a significant edge and new possibilities over conventional methods. In addition to engineering applications, DNA nanotechnology can be a link to the biomedical sciences, where it has broad applications. Cross-discipline collaborative research efforts focused on nanoparticles are showing that they have novel properties able to markedly enhance biosensing, imaging, drug delivery, and diagnostics. The author concludes that specific applications speaking to the demand of the target market are needed to push this technology out of research labs and into commercialization. As noted in other recent *Decoded* articles, however, the Supreme Court's treatment of and willingness to step into the policymaking sphere around this new technology remains uncertain. --- Shane P. Riley

---

Share This Email | Share This Email | Share This Email

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