

SHARE:



[Join Our Email List](#)



[View as Webpage](#)



July 7, 2021

Court Redirects Most Ring LLC Privacy Litigation Plaintiffs to Arbitration

"In the complaint, the plaintiffs alleged that Ring's security systems were defectively designed without sufficient security protocols, leaving users open to cyberattack, identity theft, and physical harm."

Why this is important: A group of purchasers of Ring security systems and non-purchasers who used the systems are plaintiffs in a consolidated class action against Ring that alleges the security systems were defectively designed. Ring moved to compel arbitration of all claims. The article reports on the court's recent decision, which addresses the law related to arbitration more so than technology law. The court granted the motion as to the group of purchasers and sent their claims to arbitration. Arbitration is a matter of contract, and parties are only compelled to arbitrate those claims that they agreed to arbitrate. The court found that the purchasers were on notice of Ring's terms of service, which included an arbitration clause. Their actions in maintaining Ring accounts amounted to an agreement to arbitrate their claims. Authority exists that permits a party to an arbitration clause to compel non-signatories to that clause to arbitrate their claims if certain conditions are met. The court in the Ring case apparently didn't find that law applicable. It refused Ring's motion to compel those non-signatories (the non-purchaser users of Ring's security systems) to arbitration. The result is a bifurcation of the claims and piecemeal litigation where some claims will be litigated in court and some will be arbitrated. --- [Nicholas P. Mooney II](#)

He Inherited a Devastating Disease. A CRISPR Gene-Editing Breakthrough Stopped It and Intellia Hits a 'Home Run' with Gene-Editing Results, Setting Up Entire Field for a Grand Slam

"The advance is being hailed not just for amyloidosis patients but also as a proof-of-concept that CRISPR could be used to treat many other, much more common diseases."

"The results were a pretty big deal: Intellia and partner Regeneron showed for the first time that gene editing can work in a human."

Why this is important: Both of these articles illustrate advances predicted 20 years ago when human DNA was decoded. Even at that time, most of that industry was already on hold due to the death of [Jesse Gelsinger](#). Money dried up to some extent, and faith in the concept was damaged. In the past five years, science research has loosened up. The advent of CRISPR accelerated the speed and number of applications of this treatment. We began to see exciting advances in this research. The second article also demonstrates the limitation of this model. Gene-based diseases are very specific and sometimes involve more than one gene. Most CRISPR-aided treatments now aim at single genes or a couple, and very specific mutations. We must walk before we run, and this truth applies to science, as well. --- [Hugh B. Wellons](#)

Nanotechnology and Artificial Intelligence May be Valuable Components in Securing Global Food Production

"Modern agriculture is facing a range of emerging challenges, including global climate change, rapidly growing populations, more competition for space and energy, as well as declining soil quality."

Why this is important: Food insecurity stemming from modern agriculture facing a wide-ranging panel of emerging challenges has led to the United Nations estimating that 840 million people will be affected by hunger by 2030. A team of researchers working with scientists at the University of Birmingham, UK, has devised a plan of action for assessing future methods to harness AI and integrate nanomaterials into agricultural practices. One example is using nano fertilizers to specifically target crop fertility, enhance nutrient enrichment and reduce nitrous oxide emission, thus simultaneously improving crop yields while dramatically lessening the greenhouse gas emissions associated with traditional nitrogen fertilization. On the AI side, technologies can be developed and incorporated to track exact details on nutrient cycling and crop productivity to allow for targeted application of treatments with nutrients or pesticides. The real benefits will come from harnessing these two technologies together to boost and improve farming practices around the world. --- [Brandon M. Hartman](#)

Consumers File Amended Complaint in Consolidated Clearview AI Privacy Litigation

"This comes after Clearview allegedly took billions of photographs and uploaded it to their biometric database without the plaintiffs' consent."

Why this is important: Clearview AI and the companies that use its facial recognition technology are facing scrutiny not just from the privacy bar, but also from the plaintiffs' bar. A putative class action in the Northern District of Illinois alleges that Clearview AI and other companies have compromised the plaintiffs' biometric information. Though class members are located across the country, the filing in the Northern District of Illinois reflects a strategic choice. Illinois' Biometric Information Privacy Act ("BIPA"), which limits the circumstances under which individuals' biometric information can be used, has proven to be a popular (and lucrative) foundation for privacy lawsuits in the past several years—so much so that companies collecting or using biometric information, even via outside vendors, should look carefully at whether they're compliant with BIPA and the similar statutes that are cropping up across the country. --- [Joseph V. Schaeffer](#)

Supreme Court Says You Can't Sue the Corporation that Wrongly Marked You a Terrorist

"The Court's analysis of their 'standing' —whether they were sufficiently injured to file a lawsuit—reflects a naïve view of the increasingly powerful role that personal data, and the private corporations that harvest and monetize it, play in everyday life."

Why this is important: The U.S. Supreme Court recently decided which plaintiffs could assert claims when TransUnion wrongly labelled approximately 8,000 people as terrorists because they shared the same name with a person on a terrorist watch list. The Court ruled that most of those people did not suffer an injury sufficient to confer standing and permit them to sue. Only those people whose (incorrect)

information was transmitted from TransUnion to a third party would be permitted to sue. The Electronic Frontier Foundation argues in the article that this decision disappoints and fails to recognize the reality of modern day data collection where vast amounts of personal data are collected and held by interconnected sets of corporate databases. Regardless, the Court's decision held that intangible harms were sufficient to allow an individual to sue and the risk of a future harm would permit a person to sue to obtain injunctive relief. It shouldn't be forgotten that the Court's decision applies only in federal courts.

--- [Nicholas P. Mooney II](#)

More than 1/3 of Health Organizations Hit by Ransomware Last Year

"The report also found that roughly a third of organizations that had data stolen paid the ransom to recover their information, but on average only 69% of the encrypted data was restored after the ransom was paid."

Why this is important: "Be afraid, be very afraid." Okay, my quote from the remake of "The Fly," a wonderfully campy 1986 horror movie, may be over the top, but not by much. Our nation switched to a digital medical records system in 2009, and it became mandatory by 2014. That very difficult transition became even more difficult for small practices, many of which closed. This was, however, a grand plan. It could make medical records in Morgantown, West Virginia available in a matter of seconds to an emergency heart surgeon operating in Cody, Wyoming. It also allowed doctors treating patients all to access the same data. It should improve care.

This also makes such data very attractive to cybercriminals. More than one-third of all healthcare organizations were victims of a ransomware attack in 2020. Of those who paid up, they averaged getting only 69 percent of their data back! Wonder why nurses always want a full list of all your medications, surgeries, allergies, etc.? Wonder why doctors seem to ask questions that should be in the file? (Okay, the doctor might be whiffing, but...) That change in heart medication you had last year may not be on the list anymore. That severe reaction to an antibiotic may be lost. The point is that we spent billions of dollars and five years digitizing our medical records to aid in better health. Ransomware specifically, and cybersecurity breaches in general, endanger that system and your own health. --- [Hugh B. Wellons](#)

5 Recent Lawsuits, Settlements Filed Over Data Breaches

"From a former Mayo Clinic physician being sued for accessing patient data to four class-action lawsuits launched on Scripps Health after it faced a ransomware attack, here are the lawsuits and settlements over data breaches making headlines in the last month."

Why this is important: The five lawsuits highlighted in this article are representative of the types of unauthorized access that might lead to a data breach. One lawsuit is based on alleged employee misconduct, with a former physician being accused of inappropriately accessing patient data. In the others, outside threat actors are alleged to have breached the security of the defendants' systems. The takeaway here for businesses should be that the threats can come both from the inside and the outside. It is critical given the increasing prevalence and sophistication of external attacks for companies to invest in strengthening their systems and training their employees. But, it is equally critical to review controls to limit and detect unauthorized access by those same employees. As this article shows, both can lead to potential liability for the businesses. --- [Joseph V. Schaeffer](#)

Military Looks for Novel Ways to Employ 3D Printing

"The document described five goals for the technology: integrate it into the Pentagon and the defense industrial base; promote agile use; develop best practices and proficiency; secure workflows; and support collaboration across services and the federal government."

Why this is important: The Army has set a very ambitious task for its "Jointless Hull Project:" develop a 3D metal printer large enough to create a one-piece military truck exterior. This is just one example of how the Army is seeking to incorporate 3D printing technology to innovate and make more robust supply chains. Costs for military-spec parts are frequently extremely high because they are not commonly made and must be manufactured to exacting details. The Army is looking to 3D printing as a way to produce these parts at a lower cost, more rapidly, and closer to the point where the parts are needed. This

technology is potentially game-changing for humanitarian work and natural disaster response as well – the Marine Corps' Project ICON seeks to develop technology for 3D printing structures such as buildings and bridges, thus allowing for rapid on-site replacement of critical infrastructure. --- [Brandon M. Hartman](#)

As Regulatory Scrutiny Intensifies, Crypto Exchange Binance Jumps on the NFT Bandwagon

"The crackdown is the latest in an ongoing series of setbacks for the broader crypto universe that has wiped billions off the market value of listed U.S. rival Coinbase and prompted marketplace Kraken to consider postponing its own plans to go public."

Why this is important: Binance claims to be the world's largest cryptocurrency platform by trading volume. Its size hasn't let it escape controversy. Regulators in both the U.S. and UK have been investigating its compliance with anti-money laundering requirements. Despite these investigations and the corresponding bad press, Binance recently announced the launch of a marketplace where users can buy and sell digital art, music, and collectibles as non-fungible tokens ("NFTs"). NFTs have garnered publicity in the past several months with stories of people paying tens of millions of dollars for digital art and hundreds of thousands of dollars for digital real estate. For every NFT cheerleader, a critic can be found. Recent articles have reported that the volume of NFTs is slowing, indicating their popularity is waning. Binance is undeterred, and is moving forward with the creation of this new marketplace. Time will tell if the popularity of NFTs will support this new marketplace or whether this move will add to Binance's problems. --- [Nicholas P. Mooney II](#)

Sam Altman Wants to Scan Your Eyeball in Exchange for Cryptocurrency

"Among the many parts of its plan, Worldcoin has designed an orb-shaped device that would scan a person's iris to construct a unique personal identifier."

Why this is important: Worldcoin may soon distribute its cryptocurrency to everyone on earth and all you need to do to collect it is to let the company scan your eye. Sam Altman, the former president of Y Combinator and the first investor in Worldcoin, based the intention to "use cryptocurrency to spread money around equitably [and] inspired by the trendy economic theory known as universal basic income." Under the universal basic income theory, every person would receive a steady and unconditional cash payment from the government. In order to ensure that a person only receives the share to which they are entitled, Worldcoin is using a basketball-sized orb that can scan a person's iris to create a unique identifier. Worldcoin is currently testing the orb by scanning the eyes of volunteers in exchange for cryptocurrencies like Bitcoin. Alexander Blania, the head of Worldcoin, has stated that he is aware of the privacy risks inherent in its system and "will make the process as transparent as possible so users can see how the data is used." Protecting this data will be a great concern, and the real or perceived inability may limit Worldcoin's reach. While the company's success is unknown, one thing is clear: it will be interesting to see if people value their privacy over free money. --- [Kellen M. Shearin](#)

Drug Safety Testing – From Animals to "Clinical Studies on a Chip"

"The use of healthy animals to mimic patients' responses has too many shortcomings and can put drug development programs and patients at risk."

Why this is important: "Drugs kill dogs, and dogs kill drugs." That old adage illustrates an underlying problem in preclinical testing before you begin clinical (human) testing under the FDA and/or EMA. Testing drugs and other treatments on mice and rats only provide so much information. Some have tested drugs on dogs, because they have more complicated systems. Unfortunately, over time, researchers have discovered that dog systems are different from humans in critical ways, so drugs that may be safe on humans kill dogs, which creates a preclinical record that may eliminate funding or delay development of a safe drug. We test on animals to improve the likelihood of the drug being safe for humans.

There must be a better way, right? This article describes animal-free methods to test drug safety, potentially improving the predictive model and eliminating or reducing the use of animals for such research. Several different platforms are being studied, most involving in vivo (test tube, etc.) processes, often in combination with computer modeling. We may never eliminate animal testing for human drugs, but these developments could reduce that testing and also provide a better model for preclinical work. ---
[Hugh B. Wellons](#)

Thank you for reading this issue of *Decoded!* We hope you found the information timely and useful. If you have topics you would like us to cover or would like to add someone to our distribution list, please [email us](#).

[Nicholas P. Mooney II](#), Co-editor of *Decoded* and Co-Chair of Spilman's [Technology Practice Group](#)
[Joseph V. Schaeffer](#), Co-editor of *Decoded* and Co-Chair of Spilman's [Technology Practice Group](#)



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