SHARE:

Join Our Email List

View as Webpage

June 9, 2022

Welcome

Welcome to the 11th issue of *Decoded* for the year.

We are very pleased to announce that several of the firm's practice groups and attorneys were recognized in the 2022 edition of *Chambers USA*, a directory of leading law firms and attorneys published annually.

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. Considerable credence is given to the opinions of clients.

Congratulations to the firm and the attorneys for this prestigious recognition! You can click here to learn more.

We hope you enjoy this issue and, as always, thank you for reading.

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

and

Alexander L. Turner, Co-Editor of *Decoded*

The PATCH Act: Protecting Medical Devices from Cyber Attacks

By Alexander L. Turner and Brian H. Richardson

In a previous issue of *Decoded*, we discussed the alarming fact that many medical devices, including those implanted in patients' bodies, are leaving the manufacturers with known cybersecurity flaws. Due

to these known flaws, these devices are vulnerable to being hacked, and patients' personal/protected health information ("PHI") stolen; or worse, the device being held hostage in a ransomware attack. In hopes of preventing a medical disaster associated with unprotected medical devices, this year, the House and the Senate are considering companion bills intended to significantly improve security and safety for medical devices. Senate Bill 3983, the "Protecting and Transforming Cyber Health Care Act" or "PATCH Act," and the House companion, the PATCH Act of 2022, H.R. 7084, are currently under consideration in their respective Committees. The PATCH Act represents a major step forward in securing networkable medical devices, but there are significant shortcomings in the way it addresses the ever-evolving threat of cybersecurity vulnerabilities in those medical devices.

Click **here** to read the entire article.

Protecting Intellectual Property in Augmented Reality

"Both AR and VR will undoubtedly bring a whole set of novel IP issues for individuals, companies, IP practitioners and the courts."

Why this is important: Augmented Reality ("AR") and Virtual Reality ("VR") are growing in prominence and transforming the way we live, work, play, and learn. These new technologies present a unique set of intellectual property ("IP") issues that need to be addressed and even more that are yet to be discovered. AR enhances the real world with digital details--such as the yellow first down line you see on the football field when viewing televised sports. VR puts you in an entirely virtual world and is the primary technology for the metaverse. Recent applications for AR and VR run across nearly all industries, including healthcare, travel, design, education, entertainment, and sports. To protect IP in these new frontiers, players need to address patents, trademarks, and copyrights.

Filing patents for AR is similar to other technologies, however there are important differences regarding hardware and motion tracking technologies to go from 2D to 3D. There have been tens of thousands of new patent applications filed and published on such topics already, namely from large tech companies such as Microsoft, Intel, Meta, Samsung, Google, LG, and Sony. Patent litigation has already commenced, including an infringement case against HTC's Vive headset. *ESP, Inc. v. HTC Corp.,* Case No. 3:17-cv-05806 (N.D. Cal.). The court said it was a close call, but found that ESP's patents passed the Alice test, which likely will be a central issue for litigation involving AR patents. Similarly, retailers like Macy's and Bloomingdales faced litigation for their application of technologies to enable customers to "try-on" items. With a wave of AR patent filings and litigation, practitioners need to ask: how much detail or description for the claimed uses of AR will be required in the patent specification to satisfy the written description and enablement requirements of Section 112? As industry players rush to capture IP space in the virtual world, we may see a lot of thin patents.

Aside from patents, most IP issues likely will involve trademarks and copyrights. While third parties may always engage in trademark infringement, virtual trademarks can be made to appear anywhere, and advertisers have a whole new universe to plaster logos around. This practice may lead to issues of false connection and likelihood of confusion. On the copyright side, AR will add new dimensions to the concepts of fair use and derivative works. Would morphing a copyrighted work into another similar object infringe the right to create a derivative work of the copyrighted work? Or is it fair use? What if AR includes music in the background? Is it copyright infringement?

As these new technologies continue to develop, there will be an endless list of legal, social, and ethical challenges. Practitioners can expect to see more transactions and litigations as companies race to secure their virtual IP rights. **---** Alison M. Sacriponte

---

Attorneys Line Up to Take on Healthcare Breach Lawsuits, Amid Hopes of Substantial Payouts

"In some instances, entities may face multiple lawsuits filed in the same forum, or a combination of federal and state courts."

Why this is important: Statutory compliance with HIPAA after a data breach is becoming a shining beacon for a lawsuit. HIPAA requires providers to report any breaches of protected health information impacting more than 500 patients to the Office of Civil Rights, which are then posted on its breach reporting tool. As soon as the notices are going out to impacted patients, plaintiffs' firms are opening

investigations and filing suit. This is an increasing trend that is leading to multiple suits for the same breach being filed in state and federal court simultaneously. This multiplicity of suits results in increased defense costs to defend against all of these actions as your defense counsel attempts to consolidate or stay the various actions. In previous issues of *Decoded*, we have discussed that recent data breach jurisprudence is trending toward dismissing actions that do not allege an actual injury-in-fact. However, plaintiffs' counsel are continuing to evolve their pleadings to get past a motion to dismiss, and in some cases, have been successful. This ties up litigation in the courts, and many medical facilities opt to settle than to continue the fight and potentially experience a large loss in court to a certified class action. That is a financial and strategic decision that each facility must make based on the facts of their individual cases, but these settlements only encourage more suits in the future.

As costly as these suits are, non-compliance with HIPAA is not the answer. What is the answer then? Being proactive and implementing policies and procedures that prevent falling prey to the cyberattack in the first place. As we have discussed in previous issues of *Decoded*, this means intensive cybersecurity training for your staff, implementing a system that automatically notifies employees that IT is aware that they are improperly accessing files, and being aware of the latest forms of attack and hardening your system against those attacks in advance. Only by implementing a robust cybersecurity culture and having sufficient cybersecurity insurance is a medical facility able to best defeat these types of lawsuits. --- Alexander L. Turner

---

Human Genetic Engineering is Coming. We Must Discuss the Social and Political Implications Now

"Because of CRISPR's unknown risks, its use has been limited to certain applications by longstanding consensus within the scientific community, and to a lesser extent by regulatory agencies."

Why this is important: I've written a lot about gene editing, because it will change how we treat many inherited and difficult diseases. It also literally will change the broad definition of a "human," probably narrowing it in some ways that are not good for us long term. I've often referred to the movie, Gattaca, which is available now on Netflix, if you haven't seen it. Even at 25 years old, it holds up surprisingly well. This article explains how one scientist working in this industry met another scientist in China who already is making Gattaca a reality. Allegedly, the scientist in China has already used CRISPR to "adjust" twin human embryos to give them certain desired characteristics. In other words, presumably they were perfectly healthy embryos, but now they are smarter, stronger, and faster. They were inserted into a healthy young lady, and were born full-term. Here we go! The implications of this are mostly very dark and full of unintended consequences. Imagine that Olympic glory, as well as other competitions, becomes a battle of genetic manipulation. There is no test for that! Imagine that, perhaps in addition to the SAT, your genes become a criteria for college, jobs, etc. That does not describe a world that favors equal opportunity for most people, even in the same country. --- Hugh B. Wellons

---

The Estée Lauder Companies' Virtual Try-on Targeted by Lawsuit

"While Estée Lauder's virtual try-on tool, powered by YouCam, offers a link to the company's privacy policy, that material does not disclose that 'the makeup company collects, captures, possesses or otherwise obtains consumers' sensitive biometric data.'"

Why this is important: Many businesses are turning to technology to improve a consumer's experience with their products. The Estée Lauder Companies, Inc. utilized facial scan technologies to offer virtual tools to allow potential customers the opportunity to try the products from the comfort of their home. In a recent lawsuit filed in the U.S. District Court, Southern District, the plaintiff, Celia Castelaz, alleges that Estée Lauder failed to disclose the collection of the biometric facial scan data in the company's privacy policy. The lawsuit seeks to cover all of the consumers whose biometric information was captured by Estée Lauder and who resided in Illinois within the past four years.

As businesses seek to incorporate technology with respect to their products and marketing plans, it is imperative that they carefully examine their privacy policies and consumer disclosures. They must ensure that they are clearly articulating what type of data will be collected and how such information will be maintained and stored. Consumers should be wary of readily providing personal information without having a proper understanding of the access that they are granting to third parties. --- Annmarie Kaiser Robey

Employees Cause More Cyber Breaches in Healthcare than Other Industries, Report Finds

"Employees were responsible for 39% of healthcare breaches last year."

Why this is important: Above, we discuss the fact that healthcare-related data breaches are creating a new legal industry for plaintiffs' attorneys in the form of ever increasing data breach litigation. HIPAA reporting requirements make identifying potential cases for plaintiffs' lawyers very easy. They only need to find one representative putative class member out of tens or hundreds of thousands of impacted patients to commence a class action lawsuit on behalf of all the impacted patients. In order to prevent these costly lawsuits, medical facilities must know where their vulnerabilities are.

Unfortunately, the danger often lurks within and they need not look further than their own employees to see where the biggest risk of a breach lies. Last year, medical facility employees were responsible for 39 percent of all healthcare-related data breaches. A lack of robust internal protocols and/or enforcement of policies and procedures unnecessarily exposes medical facilities to a cyberattack. Prevent these types of breaches, and a medical facility cuts its risk of being involved in a data breach-related lawsuit by over a third. Healthcare is more susceptible to insider breaches because of the private nature of the information involved. Employees get curious about a friend, family member, or enemy's personal health information and decide to access their files improperly. However, the recent trend in insider breaches is moving away from these types of breaches to more breaches being caused by miscellaneous errors like data misdelivery, and device or document loss. How does the facility protect against this? Training and enforcement. Employee training regarding who is permitted to access patient files and when, policies and protocols about ensuring that protected health information and personal identifiable information is not inadvertently sent to the wrong person, robust enforcement of those policies and procedures through periodic audits, and requiring the use of robust password protection on all devices will prevent these unforced errors that endanger patient data. These simple steps to prevent careless mistakes can cut a medical facility's risk of being involved in a data breach lawsuit by almost 40 percent. --- Alexander L. Turner

Verily Advances Smartwatch Toward Parkinson's Clinical Trial Use After Validating Technology

"Scores on the smartwatch-based virtual motor exam differed depending on whether the subjects performed the test at home or in the clinic, leading the researchers to argue that remote testing gives a more complete, accurate picture of the severity of the disease."

Why this is important: This article explains how a smartwatch/wearable device seems to be effective in diagnosing some early-stage Parkinson's cases. This is a new accomplishment for such devices (which already often recognize a number of cardiac problems). Some early-stage Parkinson's cases have very minute tremors in the arms and hands. This device does not pick up other early-stage Parkinson's symptoms. Like other manufacturers, and possibly after FDA verification, Verily must be very careful about what and how it advertises. Liability for failure to diagnose this could be high, but if Verily's findings are independently confirmed, and it is careful about what it promises, it may be clear. --- Hugh B. Wellons