SHARE:

Join Our Email List

View as Webpage

October 27, 2021

Nature of Patents and Patent Rights

By William P. Smith

When a patent is issued under the seal of the United States Patent and Trademark Office, it is signed by the Director of the USPTO or an Office official. The patent contains a grant to the patentee, and a printed copy of the specification and drawing is annexed to the patent and forms a part of it. The granted patent confers "the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States." The term of the patent is 20 years from the date on which the application for the patent was filed in the United States or, if the application contains a specific reference to an earlier filed application, from the date of the earliest such application was filed. The patent term is subject to the payment of maintenance fees as provided by law.

The exact nature of the right conferred must be carefully distinguished, and the key is in the words "right to exclude" in the phrase just quoted.

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

US Gov't will Slap Contractors with Civil Lawsuits for Hiding Breaches

"The Civil Cyber-Fraud Initiative mandates data-breach reporting for gov't contractors."

Why this is important: A company that is a victim of a cyberattack and data breach may not want to report it because of the actual or perceived damage to the company's reputation. If the company is a federal contractor, failing to report a data breach is no longer an option. The DOJ will now use its civil enforcement tools by way of the False Claims Act to punish federal contractors who do not follow accepted cyber security standards. By utilizing the False Claims Act, the federal government can also protect whistleblowers and provide them with a financial incentive in the form of the percentages of recovered damages for alerting authorities to companies that have deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches. That is why it is imperative for federal contractors to have robust cybersecurity protocols in place before a data breach occurs, and if a

breach does occur, to have effective data breach procedures already in place to accurately and quickly report the breach. Even if your company is not a federal contractor, it is still a good idea to have these policies and procedures in place to protect the company because the cost of a data breach keeps rising. --- Alexander L. Turner

---

Polygenic Screening of Embryos is Here, but is It Ethical?

"The nonprofit California-based organisation the Center for Genetics and Society has called its use here 'a considerable reach by the assisted-reproduction industry in the direction of techno-eugenics'"

Why this is important: If you are a steady reader, you've read our warnings about Gattaca here before. This is not that. This is the step before that. In IVF (in vitro fertilization), an egg is fertilized by sperm in a test tube or somewhere else outside the body and then later inserted in the uterus in hopes that it will stick and become a fetus (and later a baby). In this process, in order to increase the likelihood of success, several human eggs are fertilized, if possible, and the apparently healthiest ones are inserted or frozen for later use. This is why IVF results in multiple pregnancies (twins and triplets) more often. This polygenic screening allows any embryos produced to be tested for a variety of genetic problems (preimplantation genetic diagnosis or "PGD"), so the parents can select only the healthiest embryo(s) for implant. As this process develops and expands, more and more embryos will not meet standards. The genetic quality of humans may increase, for those who can afford it. For those predisposed to diabetes, depression, and other "markers," well, we will have fewer in the future. --- Hugh B. Wellons

---

Potential Starbucks Partnership Shows Amazon's Ambitions for Its Cashierless Retail Technology

"The co-branded stores would let people buy beverages, baked goods and hot foods without going through a traditional checkout, the report says."

Why this is important: Amazon Go grocery and convenience stores are already operating in Chicago, New York City, San Francisco, Seattle and the United Kingdom. This checkout-free shopping model uses technology to detect when products are taken from or returned to the shelves and the information is retained in your cart on your electronic device. According to the Insider news site, Amazon and Starbucks have discussed a co-branded store that would use the "Just Walk Out" technology to allow consumers to purchase beverages and baked goods using an app. Amazon and Starbucks products would be paid for separately. Although it is unclear if the partnership will proceed, this latest potential collaboration shows there is great interest in expanding the cashier-free system not only within Amazon stores, but potentially with other businesses. However this new technology is expanded, it is clear that businesses are evaluating their business models to streamline processes and improve the experience of their consumers. --- Annmarie Kaiser Robey

---

Scientists Create Strange Material that Can Both Move and Block Heat

"Researchers measure an astonishing coefficient of 900 for different heat flows."

Why this is important: This wonderfully geeky article describes a new nanoparticle that has properties to both move and block heat. Aligned just right, it might increase the efficiency and decrease the cost of exhausting heat from many surfaces, especially in computing and electronics. A few years off, this may revolutionize manufacture of many electronic devices, especially batteries. --- Hugh B. Wellons

---

Senate Hearing Opens the Door to Individual Lawsuits in Privacy Legislation

"Maureen Ohlhausen and Morgan Reed both opened the door to an industry support for a narrow private right of action that both protects consumers and prevents nuisance lawsuits, especially against small businesses."

Why this is important: On September 29, 2021 at a Senate Commerce Committee Meeting, major industry leaders supported, to the surprise of many, adding a carefully tailored private right of action to a federal privacy law. There appears to be recognition that the availability of private causes of actions for actual damages may serve as appropriate deterrents for egregious or repetitive bad privacy practices, though there was minimal support for the type of nominal statutory damages and attorney's fees often available in consumer protection legislation. A cure period or a timeframe during which a company could remedy privacy violations to insulate itself from suit was also favored. While this discussion signals progress in this arena, several significant hurdles remain to overcome on the path to a passable bill, most notably how to address federal preemption of state law. --- Risa S. Katz-Albert

---

When It Comes to Biometrics, are Our Bodies the Best Tool to Protect Privacy? and Woman Finds Amazon has Thousands of Recordings of Her - All from Home Devices

"In a world of deepfakes and regular headlines exposing how some biometrics can be beaten or confused, is biometrics the future of identity?"

"The TikTok star found that Amazon had huge folders full of audio clips of her voice, a full list of contacts from her phone, her location, and said she is 'not totally comfortable.'"

Why this is important: First, see the discussion in the second link to this article of the woman of whom Amazon has hundreds of voice recordings. If you have one of "those" devices - Siri, Google Now, Amazon Echo/Alexa, Cortana, Facebook M, Braina, etc. - Amazon or someone else may have hundreds of recordings of you! Apple probably has one of your fingerprints. Anyone else who you sign into by fingerprint has that. Ever throw away trash you have handled? Of course! It is easy (although possibly messy) to get your fingerprints. Red Cross and others may have your blood. DNA? You or any sibling ever get that checked by Ancestry.com, 23AndMe, etc.? Our biometric data is the most personal identifier we have. And for some of us, others have this already. This article discusses why passwords, if they are good, still can be an important part of this security equation. --- Hugh B. Wellons

---

Data Breach Numbers, Costs and Impacts All Rise in 2021

"A recent report found that the average cost of a data breach rose to $4.2M per incident this year."

Why this is important: What is the average cost of a data breach in 2021? A recent study found that the average cost of a data breach is now $4.24 million, the highest it has been in 17 years. Remote work and healthcare breaches are two of the leading causes of the increased cost of a breach. The leading approaches to reduce these costs are the adoption of AI, security analytics, and encryption. Companies that adopted these preventative measures saved between $1.25 million and $1.49 million compared to companies that did not adopt these measures. However, even though not every company has the ability to implement these approaches, there are steps that companies can take to lessen the financial burden of a data breach. The most important step is to have adequate cybersecurity protocols in place to prevent a data breach. The other is to have sufficient cybersecurity insurance in place to cover the actual cost of a possible breach. Insufficient insurance coverage in the face of even a minor breach can result in the company needing to pay tens to hundreds of thousands of dollars to investigate and properly report the breach. --- Alexander L. Turner

---

How Nanotechnology Will Help Us Probe the Brain in Unimaginable Detail

"The key to bridging this gap is the emerging field of 'NanoNeuro,' say the authors of a new paper in Nature Methods."

Why this is important: Our last edition of *Decoded* linked to an article explaining new, non-pharmaceutical methods for treating mental illness. This article explains how nanotechnology can help map individual brains and explain, and possibly treat, various medical problems in the brain. The science still is new, but nanotechnology, in particular, shows much promise for this diagnosis and treatment.
--- Hugh B. Wellons

Cryptocurrency Exchange Fees are a Mess. Will They Ever Improve?

"You'll never really know the exact amount until you're ready to lock and load."

Why this is important: This article highlights some of the exchange fees users pay when transferring cryptocurrencies either between themselves or to or from fiat money. If you're new to crypto investing, this is a good article to get an introduction into some of the fees, though part of it may go beyond a simple explanation. The article also discusses the difference between centralized and decentralized exchanges, gas fees, and the benefit to buying currencies on PayPal. --- Nicholas P. Mooney II

Gene Therapy is Coming of Age

"Various approaches are approved for treating blood cancers and a few rare disorders—they may soon become standard care."

Why this is important: This article explains generally the development in gene therapy. It is not earth-shattering, but it is a good general discussion. Initially, gene therapy aimed at one gene. It is expanding to multiple genes. This is critical to treat most unwanted conditions, but some of these genes have other purposes. That makes this treatment more challenging. Also, gene therapy, as we have discussed in these pages, sometimes does not last as we expect it to. We will see more of it. It will treat conditions that we could not imagine treating before. This will not, however, be a smooth ride. --- Hugh B. Wellons

---

Senators Call on Facebook to Shelve Novi Cryptocurrency Project

"'Facebook cannot be trusted to manage a payment system.'"

Why this is important: The Facebook whistleblower and Cambridge Analytica scandal haven't been forgotten. Three Senators recently sent a letter to Facebook asking it to shelve its plans to pursue a digital currency, saying it "cannot be trusted to manage a payment system or a digital currency when its existing ability to manage risks and keep consumers safe has proven wholly insufficient." Facebook is a popular punching bag nowadays, possibly for good reason. Despite the letter, Facebook said it still plans to launch its currency "as soon as it receives regulatory approval." In addition to the news and criticism about Facebook, the Senators' letter is significant for another reason: it stated their view that stablecoins generally "are incompatible with the actual financial regulatory landscape." This position will play out in the near future as central bank digital currencies continue to be developed, cryptocurrencies gain more acceptance, and more thorough regulation of the space becomes more imminent. --- Nicholas P. Mooney II

Anatomy of a Medical Device Recall: How Defective Products Can Slip Through an Outdated System

"'It truly is like we are operating in about the 1950s,' one consultant noted of the process."

Why this is important: The recall process for defective medical devices is a mess! It often works slower than recalls on consumer products, including cars. We must change this as soon as possible. This article explains that. --- Hugh B. Wellons

---

Will a Software Bill of Materials Help or Hurt Medical Device Cybersecurity?

"President Biden's cyber executive order calls for SBOMs, while FDA wants to require premarket submissions to have an inventory of third-party device components."

Why this is important: If you or a loved one use or expect to use a medical device, this should interest you. The U.S. government is trying to dive much deeper into how and why a medical device works. The concern is understanding threats from cybersecurity breaches. We already have had pacemakers and other devices temporarily compromised. Medical device companies and makers of subcomponents have been victims of phishing/ransomware attacks. Also, since many medical devices qualify for abbreviated FDA review under Section 510(k) of the Food, Drug and Cosmetics Act, many are concerned that medical devices are particularly vulnerable. The FDA cannot understand something that it doesn't see (for example, all related software). All that is true. It also is true that state-of-the-art software developed by some of these companies is beyond the ken of any FDA employees. This will require a lot of reeducation of FDA software engineers. In addition, it is true that identifying suppliers of subcomponents of medical devices in a way that is publicly accessible creates an easy shopping list for all these bad actors. This makes sense only if the government agencies make certain that this additional information does not fall prey to the same bad actors we want to thwart. Difficult problem, and an interesting article. --- 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 Chair of Spilman's Technology Practice Group

and

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