SHARE:

Join Our Email List

View as Webpage

December 8, 2021

Athletic Fashion Dispute in Race to Courthouse

By William P. Smith

Lululemon and Peloton are suing each other over clothing design patents and trade dress. Specifically, the case involves designs for athletic bras and leggings. Peloton won the "race to the courthouse" in response to a cease and desist letter from Lululemon's counsel. It initially filed a declaratory judgement action for non-infringement in the Southern District of New York on November 24, 2021. Lululemon then filed its complaint for infringement of several design patents and trade dress in its bra and legging designs. Procedurally, expect to see the cases consolidated in New York.

Click **here** for the full article.

The Cost of a Data Breach Goes Beyond the Bottom Line

"For example, ransomware attacks cost an average of $4.62 million."

Why this is important: A cyberattack can cost a company, on average, $4.62 million. That is why it is so important that every company has adequate cyberattack insurance. However, the cost to your company could go far beyond the financial cost directly associated with the breach. If your company is publicly traded, and your IT department failed to identify leadership of a known vulnerability that results in a breach, then your company may be subject to an SEC investigation and fine. There are also the reputational damages and possible loss of future business as the result of a cyberattack. There are proactive ways to protect against both the direct and indirect costs associated with a cyberattack. One way to protect against these costs is to implement a zero trust framework for your company's computer network. Another strategy is the utilization of security automation, which has been shown to save, on average, $3.81 million in cyberattack-related costs. The utilization of security automation also shortens the amount of time it takes to identify and contain a breach. Additionally, the utilization of a hybrid cloud instead of a public or private cloud can reduce breach-related costs by up to 28.3 percent. Therefore, a strong proactive approach to cybersecurity now can save a lot of financial and reputational costs in the future. --- Alexander L. Turner

---

Google Warns Crypto Miners are Using Compromised Cloud Accounts

"Google said 86% of 50 recently compromised Google Cloud accounts were used to perform cryptocurrency mining."

Why this is important: Generally speaking, cryptocurrency mining requires large amounts of computing power. Google recently discovered that threat actors have started compromising Google cloud accounts for the purpose of using those accounts to engage in crypto mining. In the majority of cases Google discovered, mining software was downloaded within 22 seconds of the account being compromised. It also discovered that around 10 percent of the compromised accounts it studied were used to scan public resources on the internet to identify other potential compromise targets. Another 8 percent were used to attack other targets. The threat actors were able to compromise the accounts because they either lacked a password or had a weak password. Others were compromised due to vulnerabilities introduced when the owner installed third-party software. At bottom, this article gives us another reason to consider our password management and to stop and think before downloading third-party software. --- Nicholas P. Mooney II

FDA Clears AFib Notification on Apple Watch

"The apps analyze pulse rate data collected by the watch's PPG sensor to identify episodes of irregular heart rhythms consistent with AFib."

Why this is important: Apple has received clearance from the FDA to include a feature designed and advertised to notify wearers of irregular heartbeats. The FDA found the accuracy of the Apple feature to be comparable with other devices sold legally for the same purpose. What is notable with the Apple feature is that it interfaces with applications that other medical technology frequently bypasses, creating the possibility that unique and identifiable private medical information about an Apple watch user will be compiled and stored digitally in one place. This is a vulnerability to users' privacy interests, as devices connected to the Internet of Things are more likely to become compromised than other devices. Additionally, privacy policies relating to the stored data become more critical, as the data collected could be valuable for healthcare development, research, or other modeling, and most consumers lack a solid understanding of how their data is being used. There are additional questions surrounding the feature relating to how consumers will comprehend the service -- it is not intended as true medical advice and the absence of a warning is not considered indicia that the user is healthy, but small print liability limitations can sometimes lead to big litigation headaches later. --- Risa S. Katz-Albert

---

Tolkien Estate Blocks Use of US Cryptocurrency 'JRR Token'

"Representatives of the Tolkien estate said the product, which was launched in August 2021, infringed the trademark of the world-famous author."

Why this is important: Cryptocurrencies, such as Dogecoin, Bitcoin, and Ethereum, to name a few, are becoming increasingly more common and are seen as a potential legitimate source of currency by society at large. However, the numerous options of what cryptocurrency to purchase serves as a significant issue to the legitimizing of cryptocurrency. Consumers who are unfamiliar with cryptocurrency and its inner-workings might see a story such as this, in which the domain was removed and operations suspended (thereby vitiating the worth of the currency) and choose to not purchase cryptocurrency in the future because the currency might become worthless. This author argues that, to convince the larger public to consider and eventually purchase cryptocurrency, there should be two to three legitimized, regulated cryptocurrencies. With regulated cryptocurrencies, the public will be reassured of the stability and legitimacy of the currency. --- Alyssa M. Zottola

---

This Company Tapped AI for Its Website—and Landed in Court

"Under pressure to make their sites accessible to visually impaired users, firms turn to software."

Why this is important: This article and a lawsuit it reports on show the limitations in artificial intelligence that society is encountering and will need to resolve. The World Wide Web Consortium, also known as W3C, develops web standards. It prepared guidelines for best practices for websites to accommodate people with visual impairments. Some companies have turned to consultants who deploy AI to translate the visual aspects of a company's website into spoken words. However, the degree to which that AI is accurate varies among websites and consultants. The article reports on one example of an image of a model wearing a white dress for sale on an e-commerce site. One of the consultant's AI technology described that image as "grass nature and summer." In another example, the plaintiff, a visually impaired man, visited the website of an eyewear retailer. The website's AI, which it purchased through a third-party consultant, translated images on the website. However, it apparently did so poorly. The plaintiff alleged that the translations were so ineffective that the retailer failed to provide visually impaired people equal access to its services. The parties ultimately reached a settlement in which the retailer denied any wrongdoing. The article doesn't discuss the amount of any settlement payment to the plaintiff, but it does note that the retailer agreed to retain the services of a new consultant and to dedicate members of the its staff to address access to its website for visually impaired people. --- Nicholas P. Mooney II

Patients File Lawsuits in Wake of Healthcare Data Breaches

"Some hospitals are successfully putting a stop to lawsuits filed in the wake of healthcare data breaches, claiming a lack of real injury to patients."

Why this is important: Cyberattacks are on the rise. This includes attacks on hospitals and other healthcare providers. The risks of a cyberattack on a hospital or healthcare provider go beyond identity theft or financial theft. A cyberattack on a healthcare provider endangers patients' protected health information ("PHI"). Cyberattacks on healthcare providers involve HIPAA, and depending on the size of the data breach and the information accessed or stolen, HIPAA may require the affected healthcare provider to provide notice of the breach to patients. The result of a HIPAA breach notice is often a lawsuit for failure to adequately protect PHI. However, healthcare providers who have been named in these types of lawsuits have seen success lately in court defeating against these claims. This includes the dismissal of claims and the decertification of a class in a class action because while there was a breach, the plaintiff could not show an injury-in-fact as a result of the breach. Therefore, the fact that a breach occurred is not enough to support a claim or a class, there must be more, and the breach must result in an actual injury to the plaintiff. --- Alexander L. Turner

---

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*