SHARE:

Join Our Email List

View as Webpage

Issue 11, 2020

Brexit Effects on Trademarks Beginning January 1

By William P. Smith

Trademark owners with registrations in EU where the UK is designated should soon receive notification for treatment of registrations and applications following the Brexit transition period. The Brexit transitional period, during which EU laws and rights have continued in force in the UK, will end on December 31, 2020. Thereafter, EU Trade Mark and Design applications and registrations (and designations of the EU) will only cover the remaining 27 EU member states.

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

Senate Passes IoT Cybersecurity Bill

"The Senate by unanimous consent passed legislation to mandate certain security requirements for internet of things devices purchased by the federal government, moving forward legislation that had been stalled on Capitol Hill since 2017."

Why this is important: Has Amazon's Alexa or Apple's Siri ever jumped in uninvited to one of your conversations? Have you been wondering just what information your connected devices are collecting and how secure it is against outside intrusions? You're not alone. The proliferation of connected devices, known by the collective term Internet of Things or IoT, has caused consumers and businesses alike to evaluate their privacy and security implications, going so far in some cases as to ban them from the premises. Congress, too, has been considering this issue for IoT devices owned or controlled by the federal government and, this November, adopted the Internet of Things Cybersecurity Improvement Act of 2020. If signed by the President, the Act will require the Director of the National Institute of Standards and Technology ("NIST") to publish standards and guidelines for IoT devices owned or controlled by federal government agencies, with an emphasis on identifying and managing security vulnerabilities. Specific considerations that the Director of NIST must make are for secure development, identity management, patching, and configuration development. Once complete, the Director of the Office of Management and Budget will be required to evaluate existing IoT devices owned or controlled by the federal government against those standards. A five-year review and revision cycle is also required under the Act. If adopted, the Act will require IoT device manufacturers to evaluate their products against this

new set of standards, with the potential for carryover into products also marketed to consumers. --- Joseph V. Schaeffer

---

Moderna Says New Data Shows Covid Vaccine is More than 94% Effective, Plans to Ask FDA for Emergency Clearance

"The announcement means some Americans could get the first doses of Moderna's two-dose vaccine within a few weeks."

Why this is important: Pharmaceutical company Moderna announced on Monday, November 30, that it will seek emergency use from the FDA for its COVID-19 vaccine. Coupled with rival Pfizer's same request on November 20, there are now two COVID-19 vaccines on the fast-track to final steps for approval before becoming available to the public. Key statistics included in Moderna's analysis show an estimated vaccine efficacy of 94.1 percent and an apparent prevention in the volunteer group of severe sickness from contraction of COVID-19. If these statistics hold true in wide-scale vaccinations, Moderna's vaccine will prove an immeasurably valuable tool in combatting COVID-19 by reducing the number of patients needing life-sustaining treatment such as being placed in ICU care or on ventilation. While FDA emergency use is not full approval, and comes with limitations as to who may receive the vaccine, these key steps will increase our arsenal of weaponry to combat the current wide scale surges in COVID-19 cases. --- Brandon M. Hartman

---

The Supreme Court Will Hear Its First Big CFAA Case

"The Supreme Court will hear arguments in a case that could lead to sweeping changes to America's controversial computer hacking laws — and affecting how millions use their computers and access online services."

Why this is important: People who blindly accept terms of service and user agreements on their computers and internet-connected technology may want to pay attention to the Supreme Court's opinion in *Van Buren v. United States*. The Supreme Court has been tasked with interpreting what the word "unauthorized" means in the Computer Fraud and Abuse Act ("CFAA"). CFAA was originally enacted to prevent hackers from gaining "'unauthorized' access to a computer or network. However, the ambiguity of the meaning of "unauthorized" has broadened the ambit of the statute. For example, Aaron Schwartz was facing 13 felony counts after using MIT's computer system, without authorization, to download scholarly articles. While this is technically unauthorized access, most people would not describe Schwartz as a hacker. Additionally, CFAA has prevented security researchers, people who "hack" into a company's computer system in an effort to discover and disclose weaknesses, from discovering deficiencies in a company's computer security even though they were encouraged to do so by the company they were "hacking." While a broad interpretation of "unauthorized" could criminalize "violating a site's terms of service to logging into a system that a person has no user account for," it is unlikely that the Supreme Court will favor an interpretation that would lead to such an absurd result. However, we may want to start paying more attention to what we do on our computers just in case. --- Kellen M. Shearin

---

Cyber Consulting Firms Get Tied Up in Post-Breach Lawsuits

"Cybersecurity consultants could be on the hook for data breaches at companies they contract with after two recent court rulings in consumer class actions."
Why this is important: Two recent court decisions raise alarming issues about the extent to which plaintiffs in lawsuits can obtain information about the work cybersecurity consultants perform for the defendants they are suing and whether the consultants can be on the hook for data breaches. In a lawsuit against Capital One, a class of consumers brought claims over a hack that exposed the data of about 100 million people in the U.S. The consumers sought a copy of the post-hack report generated by Capital One's cybersecurity consultant, and the court ruled that they were entitled to have it. In another lawsuit, a court ruled that the consultant who implemented the cybersecurity policies for Marriott hotels will face a lawsuit brought by consumers alleging negligence after a hack of its Starwood hotels exposed guest data. Two casualties of these court decisions can't be ignored. First, they create a chilling effect on what company officials may be willing to divulge to cybersecurity consultants if there's a possibility the information may find its way into a report that ultimately is ordered to be given to plaintiffs in a lawsuit. Second, the cybersecurity consultants may have to hedge their dedication to the companies that retain

them and consider their own self-preservation if the consultants themselves are open to a lawsuit for the work provided to those companies. --- Nicholas P. Mooney II

Amazon Wins Legal Fight Against eBay Over Alleged Seller Poaching

"eBay alleged that Amazon sales representatives were told to create and use eBay accounts to access the company's internal messaging system for members to solicit 'many hundreds' of eBay vendors to sell on Amazon."

Why this is important: eBay won the battle but lost the war in its litigation against Amazon. First, eBay sued Amazon in October 2018 in California state court alleging that Amazon was poaching sellers by using eBay's private messaging system that is intended for communications between buyers and sellers. In July 2019, eBay filed suit against Amazon and three of its managers in California federal court asserting that Amazon managers engaged in a scheme targeting eBay's business that violated the Racketeer Influenced and Corrupt Organizations Act ("RICO"). Amazon responded to both suits by petitioning to move the claims to arbitration, which is mandated by eBay's broad user terms and conditions, and the Court agreed. Last week, the arbitration panel found that use of eBay's private messaging system to encourage buyers to sell on Amazon's platform may have constituted a breach of eBay's terms and conditions, but eBay suffered no damages as a result. Buyers can elect to sell on both platforms, so selling on Amazon did not harm eBay. The win is significant to Amazon because it comes at a time when Amazon is under scrutiny for potential antitrust implications given the company's market reach. The case also has significant legal implications concerning website user terms and conditions. eBay sought to litigate its claims in state and federal court proceedings, but found itself pleading its cause before an arbitration panel because its own terms and conditions were written so broadly that they covered even RICO claims asserted by eBay. Moreover, eBay proved a breach of its user terms and conditions, but recovered nothing because the breach resulted in no financial harm. --- Lori D. Thompson

---

Massachusetts May Become First State to Ban Police Use of Facial Recognition

"Massachusetts lawmakers passed a police reform bill that bans public agencies and law enforcement from using facial recognition, bringing it one step closer to becoming the first state to ban the technology as privacy and civil rights advocates increasingly object to its use."

Why this is important: Facial recognition technology has become a flashpoint in the area of privacy and civil rights, and governments are responding to advocates' demands for restrictions. Several cities, most notably San Francisco and Boston, have adopted bans on facial recognition technology. And, just yesterday, the Massachusetts General Court (the Commonwealth's legislature) sent a police reform bill to Governor Charlie Baker that includes a broad ban on the use of facial recognition technology by public agencies and law enforcement. Although identified in many news reports as a first-in-the-nation bill, this legislation actually follows close on the heels of a de facto ban adopted by Vermont in the guise of a moratorium. The underlying sentiment, however, is accurate: Massachusetts is at the vanguard of this issue, and it remains to be seen how many other states will follow. --- Joseph V. Schaeffer

---

Next Biometric Identifier? 3D Images of Your Finger Veins

"'Since no two people have exactly the same 3D vein pattern, faking a vein biometric authentication would require creating an exact 3D replica of a person's finger veins, which is basically not possible.'"

Why this is important: The Department of Biomedical Engineering at the University of Buffalo has developed a new, more secure method of biometric authentication. Fingerprinting was one of the earliest methods of biometric securitization, and it has been commonly used in many different consumer technologies such as smartphones and laptops. However, hackers and fraudsters have developed ways to fake fingerprints of others in order to access protected information. Researchers at UB have now developed technology that can authenticate a person's identity by scanning a 3D image of their finger veins rather than simply a fingerprint. According to the UB research team, "faking a vein biometric authentication would require creating an exact 3D replica of a person's finger veins, which is basically not possible." The importance of data protection and secure storage of information is increasingly important

as society relies more heavily on technology to function efficiently. Protective measures must become more sophisticated and secure in order to protect consumer information, and this new technology could be a major step toward that end. --- P. Corey Bonasso

---

Biometrics Privacy Class Actions Increase This Year

"This year has already seen at least 58 BIPA complaints, nearly half of which are complaints against Tik Tok Inc. and ByteDance Inc. for their collection of face templates and voiceprints, allegedly without consent."

Why this is important: There is an increase in litigation under the Illinois Biometric Information Privacy Act ("BIPA") and the lessening of the requirements for plaintiffs to bring BIPA claims. While only 10 federal court complaints were filed under BIPA in 2018, in 2019 that number rose to 28. This year, there have been nearly 60. Recent court decisions are adding fuel to the BIPA lawsuit fire. One state court decision held that a person meets the definition of an "aggrieved person" who can bring a lawsuit under BIPA even if that person doesn't allege any actual damages. More recently, a federal court decision echoed that ruling, finding that such a person has suffered an injury-in-fact (a prerequisite for federal court standing to bring a lawsuit) sufficient to maintain a BIPA lawsuit in federal court. The issue of whether a person meets the requirements to bring a lawsuit is one of the first issues a defendant examines when it is sued. These recent court decisions will make it harder for defendants to challenge plaintiffs in that regard and, with the number of BIPA suits increasing, more companies may find themselves facing these kinds of lawsuits. --- Nicholas P. Mooney II

Revolutionary CRISPR-Based Genome Editing System Destroys Cancer Cells 'Permanently' in Lab

"The researchers demonstrated a novel lipid nanoparticle-based delivery system that specifically targets cancer cells—and co-author Prof. Dan Peer said it's the first study in the world to prove that the CRISPR/Cas9 can be used to treat cancer effectively in a living animal."

Why this is important: A first of its kind study has taken a critical step down the path to providing a radical new therapeutic treatment for cancers. Researchers at Tel Aviv University published a paper this week outlying their use of CRISPR genome editing technology in the treatment of glioblastoma, the most aggressive type of brain cancer, and metastatic ovarian cancer in mice. Utilizing the capability of CRISPR technology to identify and alter any genetic segment, the researchers were able to specifically target and disrupt the DNA responsible for the cancer cells' survival and replication with a limited number of treatments and little-to-no side effects. While noting that there is still some time before this new treatment can be used in humans, the researchers point to this line of medical technology being capable of treatment for other rare genetic diseases and chronic viral diseases such as AIDS. The long championed efficacies of CRISPR technology in revolutionizing personal medical treatments appear to now be that one crucial leap closer to realization. --- Brandon M. Hartman

---

Six Reasons Why 3D Printing is the Future

"By the year 2030 it will be unrecognizable."

Why this is important: Although 3D printing was first invented in 1983, the evolution of the technology has had a period of explosive growth in the last decade. Technology using 3D printing has high initial costs to set molds and program designs, but unlike regular manufacturing processes, 3D printing is very efficient once the programming is set. No specific molds are necessary, and injection plastic is all that is needed to produce more units after the programming is in place, which goes a long way to solving the problem of economies of scale. Furthermore, 3D printing is able to produce highly complex products, which gives it another advantage over traditional manufacturing. Units from a 3D printer are typically ready for use in two to five days, which makes it an attractive option for emergency orders of anything from healthcare products to prototypes, to regular inventory orders. Traditional manufacturing isn't likely to disappear anytime soon, but 3D printing could overtake it sooner than expected. --- P. Corey Bonasso

---

Workers' Handprint Retention Suit Moved Back to Federal Court

"An automotive supplier's retention of employees' handprints used for its timekeeping system after their employment ended constitutes an injury necessary for standing in federal court, the Seventh Circuit ruled."

Why this is important: As noted above, more companies are likely to find themselves staring down the barrel of a lawsuit brought under the Illinois Biometric Information Privacy Act ("BIPA"). Here, the plaintiff was an employee of the defendant's plant for several years but left its employ last year. During that time period, employees, including the plaintiff, were required to clock in and out of work by scanning their hands. The plaintiff represents a class of former employees alleging that the defendant maintained copies of their biometric information (their handprints) without providing them the required disclosures under BIPA about the defendant's retention of that information. --- Nicholas P. Mooney II

The Global Biometric System Market Size is Projected to Grow USD 36.6 Billion in 2020 to USD 68.6 Billion by 2025

"Major factors driving the market growth include the increasing use of biometrics in consumer electronic devices for authentication and identification purposes, the growing need for surveillance and security with the heightened threat of terrorist attacks, and the surging adoption of biometric technology in automotive applications."

Why this is important: Biometric authentication methods in consumer technology such as smartphones, computers, and even automobiles have grown in popularity over recent years, and that growth does not appear to be slowing anytime soon. Furthermore, U.S. governmental agencies are adopting biometric authentication measures to identify and reduce criminal activities. As humans develop more sophisticated technology, we have continually concluded that natural features of the human body provide the highest level of uniqueness for securing information. Fingerprints, palmprints, and eye or face scanners have had the most success in the biometric security world, but we are only scratching the surface of what is possible for biometric technology. This industry very likely will continue to grow in order to further secure consumers' private data. --- P. Corey Bonasso

---

LAPD Bans the Use of Clearview's Controversial Facial Recognition Software

"Officers will be able to use the Los Angeles County system and nothing else."

Why this is important: Clearview AI and the Los Angeles Police Department ("LAPD") are no strangers to *Decoded*. We have previously discussed a lawsuit against Clearview AI over its collection of biometric data to create its facial recognition database, as well as a lawsuit against Los Angeles over its use of location data. It's unclear what effect these lawsuits had on the LAPD (if any), but it seems that lobbying by privacy and civil rights advocates is having an effect. Shortly after being informed that some of its employees were accessing Clearview AI's database to perform searches, the LAPD placed a moratorium on its use. This does not mean that LAPD will no longer employ any facial recognition technology at all—it will continue the use of its own databases—but it does halt the use of third-party databases that privacy and civil rights advocates have identified as particularly problematic. --- Joseph V. Schaeffer

---