BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

TECHNOLOGY & INTELLECTUAL PROPERTY UPDATE

What Exactly Is Use in Commerce?

Many federal trademark applications are filed on an intent-to-use basis, which means that the applicant has not yet begun to use the mark in connection with its business activities to brand, market, and sell its products. However, in order to complete the trademark registration process, it is necessary to demonstrate to the Trademark Office that the mark is being "used in commerce." But what type of use is sufficient to demonstrate to the Trademark Office that a mark is being used in commerce?

U.S. law defines "commerce" for purposes of federal trademark requirements broadly as "all commerce which may lawfully be regulated by Congress." Demonstrating that a mark is "used in commerce" requires that the mark be used in the ordinary course of trade and not used merely to reserve a trademark right in the mark. So, in order to meet the "use in commerce" requirement of the Trademark Office, a mark must (1) be used in connection with commerce that may be regulated by Congress, and (2) be in general use by the business.

Determining whether the use of a mark is in connection with "commerce" that is lawfully regulated by Congress requires more unpacking. Typically, commerce lawfully regulated by Congress is thought of as interstate commerce – or the marketing or sale of goods across state lines. However, it has long been recognized that the sale or advertising of a mark solely within the boundaries of single state may also constitute commerce that is regulated by Congress. This principle has been expanded upon to include several variations of "use" within a single state that may nevertheless qualify as commerce lawfully regulated by Congress. An example of the outward bounds of such intrastate use is found in the case of Christian Faith Fellowship Church. This case involved the in-state sale of two hats to out-of-state customers. The Court of Appeals for the Federal Circuit held that these sales sufficiently constituted commerce that may be regulated by Congress by reasoning that the in-state sales, when taken in the aggregate, would affect interstate commerce.

This standard, as applied in the Christian Faith Fellowship Church case, has been adopted by the Trademark Office in its manual for examining procedures, and is directly applicable when considering whether a mark has been used in commerce. The practical implication is that demonstrating "use in commerce" may be easier may than it first appears. Businesses established and operating in a single state should thus pay particular attention to any sales or directed advertising to out-of-state consumers, as such activities may be important for establishing use of a businesses' mark in commerce.

Next month we will examine the nature and extent of use that is required to demonstrate sufficiency of use for registration purposes.

What Exactly Is Use In Commerce? Part 2

Last month (July 2018),we discussed what type of use constitutes "use in commerce" in order for a trademark to be registrable with the Trademark Office. In addition to use in connection with a type of commerce capable of being regulated by Congress, the trademark must be in general use by the applicant prior to registration. Specifically, the trademark must be in "bona fide use in the ordinary course of trade." The Trademark Office will not consider a token use, solely to reserve rights in the trademark, a bona fide use.
Typically, use of a new trademark by a business is rolled out gradually; so when does use of the mark rise to the level of bona fide use in the ordinary course of business? The Trademark Office focuses on three factors in assessing whether there is a bona fide use: (1) The amount of use; (2) The nature or quality of the transaction; and (3) What is typical use within a particular industry. See TMEP 901.02. In Automedx, the Trademark Trial and Appeal Board held that the applicant's use of the SAVE mark in connection with the sale of prototype models of its portable ventilator to the military was a bona fide use. In making this holding the Board focused on the fact that the sale of the prototypes was for the legitimate business purpose of evaluation by the customer in determining whether to buy additional models in the future. See Automedx Inc. v. Artivent Corp., 95 U.S.P.Q.2d 1976 (T.T.A.B. Aug. 17, 2010).

In contrast, the Board found in Plant Food Systems that applicant's use of the RENEW trademark in connection with one sale of fertilizer over four years was not a bona fide use. In making this determination the Board considered whether the limited use of the trademark was common in connection with the applicant's industry and whether the shipment was for commercial purposes. The Board found that the shipment was noncommercial in nature, as the shipment was to a distributor for evaluation, but the applicant could not demonstrate any evaluation analysis after such shipment. Further, there was no industry-specific reason to explain only one use of the mark in four years. For this reason, the Board found no bona fide use in the ordinary course of trade. Plant Food Systems, Inc. v. Earthrenew, Inc., No. 91194313, 2012 WL 9172068 (Jan. 6, 2012).

When evaluating whether use of your trademark is enough to show bona fide use, it is important to consider the intent behind your business's use of the mark. Particularly, if the use of your mark is primarily for obtaining a registration, it likely will not meet the factors for a bona fide use. However, limited use of your trademark for commercial purposes, such as evaluating a market or having consumers evaluate the underlying good or services, is likely a bona fide use. Overall, focusing on the commercial use of your trademark and marketing and/or selling to consumers out-of-state is key for demonstrating "use in commerce" for your federal trademark application.

AriAnna C. Goldstein

BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

TECHNOLOGY & INTELLECTUAL PROPERTY UPDATE

GDPR Enforcement Update: French Data Protection Authority hits Google with a Historic 50 Million Euro Penalty

On January 21, 2019, the French data protection authority ("CNIL") imposed a massive financial penalty of 50 Million euros (approximately 56.8 Million U.S. dollars) against Google for violating provisions of the General Data Protection Regulation ("GDPR"). The penalty is the largest to date assessed under the GDPR and indicates the severity of noncompliance. According to the CNIL, the penalty is the result of complaints filed—one of which was filed on May 25, 2018, the day the GDPR went into effect—by privacy-advocate associations None of Your Business ("NOYB") and La Quadrature du Net ("LQDN"). The complaints alleged, among other things, that: (1) Google's privacy policy and general terms and conditions (the "Policies") violated the GDPR because users were forced to consent to these policies in order to use their Android devices and such forced acceptance did not constitute valid consent under the GDPR, and (2) by merely listing several bases for lawful processing, Google's privacy policy failed to support exact data processing operations with a specific legal basis as required under Articles 6 and 9 of the GDPR. The CNIL began investigating the allegations made in the complaints on June 1, 2018.

Although Google will undoubtedly appeal and fight the CNIL's penalty, this historic enforcement action and the CNIL's opinion provides valuable insight into the following: (1) how DPAs may interpret and enforce the GDPR, (2) GDPR enforcement procedure regarding forum and jurisdiction, (3) the persuasive authority of EDPB guidance, (4) guidance regarding the transparency and accessibility of privacy policies and terms of use, and (5) guidance regarding consent and lawful bases for data processing operations.

The CNIL's opinion provides an often overlooked aspect of the GDPR—claim and enforcement procedure—by addressing how the GDPR determines which EU Data Protection Authority ("DPA") is the most appropriate to serve as the "lead authority." For organizations established in the EU, the GDPR states that the DPA of the country where the organizations' main establishment is located should be the "lead authority" (the "One-stop-shop Rule") for purposes of investigating alleged violations and enforcing the GDPR. Google argued the CNIL was the inappropriate DPA to investigate the complaints because Google's European headquarters are based in Ireland. And thus, under the One-stop-shop Rule, the Irish DPA should have been the "lead authority," not the CNIL. The CNIL disagreed with Google, noting that the GDPR, similar to the Federal Rules of Civil Procedure, seeks to prevent forum shopping and allowing Google to "pick its DPA" based on its self-designated European headquarters was akin to forum shopping. Instead, the CNIL determined that "in order to qualify as a principal establishment, the institution concerned must have decision-making power with regard to the processing of personal data in question," concluding that when the CNIL began its investigation, Google's European headquarters "did not have a decision-making power on the processing operations carried out in the context of the Android operating system and the services provided by GOOGLE LLC, in relation to the creation of an account during the configuration of a mobile phone." Because the One-stop-shop Rule did not apply, the CNIL, and the other DPAs, had the authority to investigate and render a decision on Google's processing operations.

The CNIL conducted online inspections to verify Google's data processing operations complied with the GDPR by analyzing users' browsing patterns and access to certain documents when creating a Google account during the configuration of Android-based mobile devices. The CNIL implemented the guidelines established by the European Data Protection Board ("EDPB") in its evaluation; specifically, the EDPB's "Guidelines on Transparency." The CNIL's findings provide insight into how DPAs may interpret the GDPR. First, the CNIL analyzed whether Google's Policies and the methodology used to present users with the opportunity to review such Policies (the "Methodology") complied with Articles 12 (Transparency) and 13 (Information to be Provided)—they were not. While the CNIL noted that the Policies contained the required information, "the information that must be disclosed to individuals pursuant to [Article] 13 [was] excessively scattered in several documents," and "[s]uch an ergonomic choice leads to a fragmentation of information thus forcing the user to multiply the clicks necessary to access the different documents." The CNIL used the following scenario to illustrate the overall lack of accessibility of Google's Policies:

[I]n terms of geolocation data processing, [CNIL's investigation] notes that the same course devoid of any intuitive character is required of the user with regard to information relating to geolocation data. The user will have to complete the following steps: Review the Privacy Policy and Terms of Service, click More Options, and then click the Learn More link to view the Location History page and view the displayed text. However, as this text

Continued >>>

is only a short description of the processing, the user will need to go to the Privacy Policy document and access the Information about your location to access the rest of the information.

The CNIL found that Google's Policies did not comply with the GDPR's transparency requirements because the information provided to users about how their data was collected, used, and processed was generic, "particularly imprecise and incomplete," and did not allow users to sufficiently understand the consequences of allowing Google to process their data. Ultimately, the CNIL explained that the genericity and lack of accessibility of the Policies combined with Google's "massive and intrusive" data processing operations, rendered users unable to measure the potential effect of Google's data processing operations on their private lives, let alone provide valid consent to such data processing operations.

Next, the CNIL assessed whether Google's proffered means of lawful processing—consent—complied with the GDPR. Under the GDPR, "[c]onsent is presumed not to have been freely given if separate consent cannot be given to different personal data processing operations," meaning "data controller[s] . . . seek[ing] consent for various specific purposes should provide separate consent for each purpose so that users can give specific consent for specific purposes." Google utilized an opt-out method and a series of checkboxes to obtain consent after users had already accepted Google's Policies and established a Google Account. The CNIL concluded that the timing and opt-out method did not constitute valid consent because the consent was "not given through a positive act by which the person consent[ed] specifically and distinctly" to Google's data processing operations. Regarding Google's use of checkboxes, the CNIL stated "ticking the boxes I accept the conditions of use of Google and I accept that my information is used as described below above and detailed in the privacy rules, and then selecting Create Account—cannot be considered as the expression of a valid consent."

Sean T. Nakamoto

BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

TECHNOLOGY & INTELLECTUAL PROPERTY UPDATE

What can you do to help protect yourself from data breaches?

On November 30, 2018, Marriott revealed that its Starwood reservation system had been hacked exposing the personal data of approximately 500 million guests. It appears that not only credit card information was compromised but also passport numbers, birth dates, cell numbers, arrival and departure dates, etc. The Marriott data breach is just another in a long series of seemingly continuous breaches.

Do you pay attention to the notice letters sent in response to data breaches such as Marriott, or have you succumbed to "breach fatigue"? Our strong advice is to pay attention. If you receive notice that your information was potentially involved in a data breach, carefully read the letter and seriously consider taking advantage of any credit monitoring or other services which are offered. For example, Marriott offered an identity monitoring service from WebWatcher which will alert you if your information shows up online or on the dark web. While industry experts largely agree that such monitoring services does not "prevent" identity theft and individuals must exercise constant vigilance, these monitoring services serve as an additional "set of eyes."

In addition, you should consider taking the following proactive measures:

1. Change all of your passwords—immediately. When you create new passwords, be sure to use a different one for each site. And make the password length as long as you are allowed. If the site will allow passwords of 15 characters—use all fifteen. Most experts now agree that length of a password is more important than its "complexity."

2. Use a password manager. If you follow the advice above, a password manager will become a necessity. There are a number of good ones available such as: LastPass, Dashlane, Keeper,1Pass, Roboform, LogMeOnce, Boss, etc. You can easily search online for password managers and learn about your options.

3. Implement multi-factor authentication whenever it is offered. This usually involves sending a code to your cellphone or receiving a code from an additional application installed on your smart device. As of now, it is the most widely used and most cost-effective authentication strategy available. While some users may view multi-factor authentication as a "hassle," the extra security it provides is worth the extra 45 seconds required complete the process.

4. Use PayPal, Apple Pay or a similar online payment service rather than saving credit card information in multiple online accounts. And make sure that service is protected with multi-factor authentication.

5. Unless you frequently visit an online store or vendor, use the "Guest" checkout feature rather than creating another on-line account. This will help to minimize accounts with your information that could be compromised.

Finally, before you provide any personal information online, take a moment to pause and weigh the benefits you receive for providing that information against the harm that might result if it is misused—remember, the information you put online will likely be there forever. The more you can reduce your online footprint the less you will have to worry about breaches such as Marriott.

James E. O'Connor

BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

TECHNOLOGY & INTELLECTUAL PROPERTY UPDATE

SCOTUS Decision in AMEX Case Puts Credit Card Networks in Favorable Negotiating Position with Retailers

In the latest development in the battle between retailers and the card networks over swipe fees, the Supreme Court ruled on Monday, June 25, 2018, that American Express' anti- steering rules, which prevent merchants from encouraging customers to use other card types, such as Visa and Mastercard, do not violate antitrust laws.

Stores sometimes will not accept American Express cards since American Express typically charges merchants a higher interchange, or "swipe fee," than its competitors do. When consumers buy items with their American Express cards, the credit card company charges the store an average of 2.37 percent globally. That compares to the less than 2 percent that Visa and Mastercard say they charge merchants. Given those rates, it is understandable why merchants would prefer to steer customers toward the use of Visa or Mastercard over American Express.

Justice Thomas, writing for a 5-4 majority, stated that the unique "two-sided" nature of credit card networks, in which a service provider links consumers to businesses, requires different treatment for antitrust purposes. In particular, the Court reasoned that because of their "two-sided" nature, engaging in anti-competition analysis with respect to credit card networks requires consideration of the impact on both sides of the market. By ruling in favor of American Express, the Court noted it was indirectly protecting the American Express rewards benefits offered to cardholders. Viewed that way, Justice Thomas wrote, American Express promoted competition by designing rewards programs to attract affluent customers.

"While these agreements have been in place," Justice Thomas wrote, "the credit-card market experienced expanding output and improved quality. Amex's business model spurred Visa and Mastercard to offer new premium card categories with higher rewards. And it has increased the availability of card services, including free banking and card-payment services for low-income customers who otherwise would not be served."

For its part, the dissent, written by Justice Breyer, took particular issue with the majority's apparent different treatment of so-called "two-sided" platforms, noting that the concept could be expanded to apply to several internet-related goods and services.

Notably, the Court's decision may also impact ongoing settlement negotiations between several retailers and Visa and Mastercard over their own anti-steering rules. The decision likely puts Visa and Mastercard in a stronger negotiating position than they previously were due to the Court's apparent application of a more deferential antitrust scrutiny for credit card networks. Given the Court's American Express decision, Visa and Mastercard may be unwilling to make more substantial changes to their anti-steering rules than they otherwise would have.

Eli A. Rosenberg

BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

TECHNOLOGY & INTELLECTUAL PROPERTY UPDATE

What You Need to Know About California's New Privacy Law

On the heels of the European Union's implementation of the General Data Protection Regulation ("GDPR"), on June 28, 2018, California enacted the most comprehensive data privacy law to date in the United States. The California Consumer Privacy Act of 2018 (the "Act") was quickly passed by the California legislature to secure the withdrawal of an even more far reaching measure that had qualified for the November ballot. The sponsor of the ballot initiative agreed to withdraw the measure if the legislature passed a consumer privacy bill prior to the June 29th withdrawal deadline. Given the difficulty of making any revisions to a measure enacted by initiative rather than by the normal legislative process, the legislature quickly adopted and the governor signed the Act into law in only seven days. Legislative amendments to the Act are expected before it goes into effect on January 1, 2020, and the Act also requires the California Attorney General to develop certain implementing regulations.

Who Has to Comply?

As passed, the Act is likely to affect not only many California businesses, but a large number of businesses that merely have an online presence in California. The Act applies to for-profit entities, located anywhere in the world, that do business in California, collect (or engage a third party to collect) the personal information of California residents and satisfy at least one of the following: (1) have over $25 million in annual gross revenue; or (2) buy, sell, receive or share for commercial purposes, the personal information of 50,000 or more California residents, households or devices on an annual basis; or (3) derive 50 percent or more of their revenue from the sale of personal information of California residents (any such entity that is a "covered business"). It also applies to any parent or subsidiary of a covered business using the same branding.

As written, non-profits, small companies, and those businesses that do not traffic in large amounts of personal information, and do not share a brand with an affiliate who is covered by the Act, will not have to comply with the Act.

How is Personal Information Defined?

The Act defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The Act provides a non-exhaustive list of examples that includes some expansive examples. For example, personal information includes "commercial information," including "records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies"; "Internet or other electronic network activity information," including browsing and search histories; "education information"; and "[a]udio, electronic, visual, thermal, olfactory, or similar information."

Personal information does not include the following: (1) information that lawfully is made available from federal, state or local government records that is used for a purpose that is compatible with the purpose for which such data is so maintained; (2) protected health information that is governed by the California Confidentiality of Medical Information Act or the Health Insurance Portability and Availability Act of 1996 ("HIPAA"); (3) personal information governed by the Fair Credit Reporting Act; (4) personal information governed by Gramm-Leach-Bliley Act; and (5) personal information governed by the Driver's Privacy Protection Act of 1994. The Act does not apply to de-identified personal data, as long as the de-identification measures meet the Act's very strict standards, or to aggregate consumer information, which also is defined strictly by the Act.

What Rights are Consumers Given?

The Act gives "consumers" (defined as natural persons who are California residents) four basic rights in relation to their personal information:

1. The right to know, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being

Continued >>>

disclosed or sold;
The right to "opt out" of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, the right not to have their personal information sold absent their, or their parent's, opt-in);

2. The right to have a business delete their personal information, with some exceptions; and

3. The right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.

What are the Enforcement Rights?

The Act can be enforced by the California Attorney General, subject to a thirty-day cure period. The civil penalty for intentional violations of the Act is up to $7,500 per violation. The Act also provides a private right of action that allows consumers to seek, either individually or as a class, statutory or actual damages and injunctive and other relief, if their sensitive personal information is subject to unauthorized access or disclosure as a result of a business's failure to implement and maintain required reasonable security procedures and practices. Statutory damages range between $100 and $750 per California resident per incident, or actual damages, whichever is greater.

What is the Potential Impact?

It remains to be seen whether other states will follow California's lead and adopt similar laws. If a patchwork of state laws evolve with respect to broader privacy rights like those covered by the Act, companies could be forced to navigate different (and potentially conflicting) state privacy requirements in the ordinary course of business.

Grayson J. Derrick
Chair, Technology and Intellectual Property Section

BH | BAIRDHOLM LLP
ATTORNEYS AT LAW

TECHNOLOGY & INTELLECTUAL PROPERTY UPDATE

Patent Office Revisits Subject Matter Eligibility and Addresses Certain Functional Claim Limitations in New Guidance

On January 7, 2019, revised guidance from the United States Patent and Trademark Office on patent subject matter eligibility took effect, paving the way for what many stakeholders expect to be a decrease in the number of patent claim rejections under 35 U.S.C. §101. The guidance attempts to provide a definition of "abstract idea" that is more definite than what was previously available under Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. 208 (2014), jurisprudence. Through the revised guidance, the Patent Office aims to make it easier for applicants to predict what subject matter is patent eligible, and to increase consistency in the application of § 101.

Section 101 provides that one who invents a "new and useful process, machine, manufacture, or composition of matter . . . may obtain a patent therefor," and has been the subject of much controversy since Alice, in which the Supreme Court promulgated a two-step test to determine whether a given subject matter is patent eligible under § 101. Under Alice, an examiner must decide whether a claim is directed to a "judicial exception" such as a law of nature, a natural phenomenon, or an abstract idea. If the claim is not directed to a judicial exception, the Alice analysis stops, and the invention is deemed to be subject matter eligible. If the claim is directed to a judicial exception, the Alice analysis continues with an assessment of whether the application claims additional elements that amount to significantly more than the judicial exception. If so, the claimed invention qualifies as eligible subject matter.

Consistent application of Alice, particularly in the case of an abstract idea, has become difficult because examiners, when considering whether a claim is directed to an abstract idea under the first step of the Alice test, are required to consider previously-decided examples of similar subject matter. The Federal Circuit has ruled on the subject matter eligibility of a large number of cases—and, frequently, its identification of subject matter as abstract in one case is inconsistent with its identification of similar subject matter as not abstract in another. Many applicants and practitioners are frustrated by this inconsistency because it makes patent predictability difficult—leading some to believe it allows examiners to "cherry pick" favorable precedent in order to formulate a § 101 rejection.

The new guidance attempts to reduce reliance on precedent by examiners under Alice by setting forth three categories of abstract ideas: mathematical concepts, certain methods of organizing human activity, and mental processes. If a claim recites subject matter that does not fall within one of these three categories, the claim should not be treated as being directed to an abstract idea, constituting patent eligible subject matter under the first prong of Alice. If, on the other hand, a claim recites subject matter that does fall within one of the three categories of abstract ideas, the examiner must determine whether the abstract idea is integrated into a practical application. If the abstract idea is so integrated, the claim is not "directed to" an abstract idea and the subject matter is patent eligible, again under the first prong of Alice. If the abstract idea is not integrated into a practical application, the analysis continues under the traditional Alice framework to determine whether the claim recites additional elements that amount to significantly more than the judicial exception.

While the § 101 guidance, in theory, should serve to reduce unpredictability with respect to § 101 and Alice, it is unclear if the Federal Circuit (or the Supreme Court, for that matter) will adopt the guidance as law when given the opportunity.

In addition to the revised § 101 guidance, the Patent Office also released new guidance regarding the examination of computer-implemented functional claim limitations under 35 U.S.C. § 112. The § 112 guidance requires that, when considering a functional claim drawn to computer-implemented inventions, an examiner applies the applicable presumption (based on the presence of the term "means" in the claim) and three-prong analysis under existing law, including by making a determination as to whether the claim sets forth sufficient structure for performing the recited function. The guidance also requires that, for a computer-implemented § 112(f) claim limitation, the specification must disclose an algorithm for performing the entirety of the claimed function in order to satisfy 35 U.S.C. § 112(b), including where one of ordinary skill in the art is capable of writing software that performs the function.

Continued >>>

Even where a claim is not examined as a mean-plus-function claim under § 112(f), the new guidance requires that computer-implemented functional claim language still satisfy the written description and enablement requirements of § 112(a)—and requires that the specification disclose both the hardware and the algorithms that achieve the claimed function in sufficient detail to enable one of ordinary skill in the art (i) to make and use the claimed invention, and (ii) to conclude that the inventor possessed the claimed invention.

According to the Patent Office, both guidance documents are intended to produce reasonably consistent and predictable results across applications and throughout the Patent Office. The public is invited to submit written comments regarding the § 101 guidance to Eligibility2019@uspto.gov, and on the § 112 guidance to 112Guidance2019@uspto.gov.

Patrick M. Kennedy