Internet of Things Part 3:
How Your Smart Toothbrush Is An Idea Worth Protecting

Prepared by:
Matt Acosta and Emilio Nicolas
Jackson Walker

LORMAN®

Published on www.lorman.com - November 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Internet of Things Part 3:
How Your Smart Toothbrush Is An Idea Worth Protecting

Written by Matt Acosta and Emilio Nicolas - 09/19/2018 - Insights

Let's set the scene: My new company develops a smart toothbrush from the ground up. It brushes your teeth, provides you with real-time information about your dental health while you brush, and even provides targeted advertising for dental products you may need. It's essentially your own personal dental hygienist, with a charging pod, and controlled by an app. Brilliant, I know. Suddenly, every other tech company is selling smart toothbrushes. Market share is tanking. What do I do? Do I license my product, design, technology, or software? Nope, the competing products have a different, more stylish look; and my competitors "independently" invented their own technology and wrote their own code. They don't need my toothbrush software. Do I sue? That's only an option if I have some basis and haven't taken any steps to protect my intellectual property. Do I sell the company? Probably. Am I now a millionaire? No, I don't really have any assets besides 10 pallets of toothbrushes and a 5 percent market share. Are my dreams of becoming "Big Toothbrush" crushed? Yeah.

I've noticed over the past several years that new tech companies are increasingly ambivalent to the very notion of intellectual property. On the one hand, there is a recognition that the value of these companies stems from their design and engineering prowess, i.e., their intellectual work product. On the other hand, there are varying degrees of distrust in our intellectual property system. The complaints include that IP protection is "too costly," "has no value beyond expensive litigation," and that "open

source is the way of the future." While many of these critiques are fair and deserve discussion, there is one inescapable truth: If it belongs to everyone, it belongs to no one.

Without IP protection, *your* product is also *my* product, or it easily could be. The result of *your* thousands of hours of design can be mine simply because I offer one of your enterprising engineers a company car and a matching 401(k). This stuff really happens, and more often than you might think. Also, there is a vast difference between giving away your IP for free and not having any IP protection at all. These differences tend to get muddled as the IP policy debate rages on. And the distinction makes a difference in the present "open source" debate, or in other words, whether I should distribute my technology for free.

Within each new IoT device lives some type of intellectual property. The big question is whether that property can be protected, and if so, how? The next question is often, is it worth it? Astonishingly, many companies don't ask these questions until it is too late. Like everything else in business, IP protection needs a strategy. Especially in the rapidly expanding IoT market.

Several surveys have concluded that many small- and medium-sized tech companies lack even a basic understanding of IP and its role in their industry (See *What Young Innovative Companies Want: Formulating Bottom-Up Patent Policy for the Internet of Things*). This article clarifies some of these misconceptions in the context of the Internet of Things and provides a foundation for answering the question, does this even matter?

Are Software Patents Dead?

When most people hear "intellectual property," their first thought almost always gravitates toward patent protection. And rightly so. A patent is useful for a variety of reasons. Patent protection can help secure funding for a new

technology company. It can single-handedly boost valuations, discourage copying, and be monetized on the open market. However, the rumor has lately permeated throughout the tech industry that it is "nearly impossible" to patent inventions stemming from software.

While it is true that it is more difficult to patent software-based technology than it was 10 years ago, as it has always been, a novel and non-obvious invention is patentable. A purely abstract idea cannot be patented. Although recent law has greatly expanded what constitutes an abstract idea, that same law recognizes that sometimes even an abstract idea can be patented if it has a sufficient enough "inventive concept." The end result is that drafting and prosecuting software-driven patents requires a little bit more legal wizardry than previously.

Even so, is patenting worth the expense? Established software companies certainly think it is. Facebook owns several thousand patents. Twitter owns more than a thousand. Uber owns a couple hundred. And Rovio, the company made famous by their game *Angry Birds*, has about 40 patents and pending applications—several granted in the last year. If a purely software-driven company focused on irate chickens is successfully patenting its inventions, then perhaps it is an indication that software-driven patents might still be relevant and valuable. Moreover, there are hundreds of IoT-related patent applications being filed every month.

The largest new barrier to obtaining patent protection on any invention, be it software or devices, begs the question of whether your idea is actually "abstract" under recent Supreme Court decisions. Under long-standing law, "abstract ideas" are not patentable. The Supreme Court has developed a two-part test for analyzing patent ineligibility because of "abstractness." First, does your idea fall in an "abstract" category? (*Mayo*, 566 U.S. at 77) In step two, we ask whether your "abstract idea" has nevertheless an

"inventive concept" that is drawn to "significantly more" than a patent upon the abstract concept itself. This is often referred to the *Mayo/Alice* test, after the Supreme Court cases that established the standards.

But never fear, the Federal Circuit Court of Appeals quickly noted that "[we do not think] that claims directed to software, as opposed to hardware, are inherently abstract and therefore only properly analyzed at the second step of the Alice analysis. Software can make non-abstract improvements to computer technology just as hardware improvements can, and sometimes the improvements can be accomplished through either route." To me, this ends the argument that "software patents" are dead-on-arrival. Even the argument that software patents are *effectively* dead seems to be thin. For example, U.S. Patent No. 9,497,572 is titled "Internet of things platforms, apparatuses, and methods," and was granted in November 2016, long after *Mayo/Alice*. While the claims of this '572 Patent include physical devices, the core technology described is software-based.

Nevertheless, the practical problem faced by software-based patents is that "abstract concept" has been defined broadly to include "fundamental economic practices," "method[s] of organizing human activity," and "mathematical algorithms." This has led many software patents driven by "algorithms" to be categorized as "abstract." As a result, most of the time, we quickly move to part two of the test: Is there enough of an "inventive concept"? The legal wizardry comes by framing your idea in such a way, based on the hundreds of cases that have tackled this question, demonstrating that the idea is tied to something that is not "abstract" while making the "inventive concept" apparent to the discerning patent examiner or judge.

This distinction can be *very* thin. For example, the Federal Circuit determined that a patent directed to systems for advertising on mobile

devices was not patent eligible because the invention could be described at its most simplistic as "streaming content generally." The fact that the patent was restricted to mobile devices did not matter. On the other hand, that case was distinguished by a Delaware court that found a patent covering software for vibration feedback on a mobile device was patentable—even though I could easily simplify the invention as "receiving a confirmation (a buzz vibration) when operating buttons on a touchscreen." The court said that this invention was tied to improving a "portable device." According to the court, the distinction was that, in the earlier case, software was not "improving" the device, while the latter software was.

If these distinctions seem a bit vague, you are not alone. The new Director of the U.S. Patent & Trademark Office is on record as saying "our current law surrounding patentable subject matter has created a more unpredictable patent landscape that is hurting innovation and, consequently, investment and job creation. Recent cases from the Supreme Court . . . have inserted standards into our interpretation of the statute that are difficult to follow. Lower courts applying these cases are struggling to issue consistent results." This current landscape requires more thought and strategy in crafting solid patents for the thousands, if not millions, of inventive concepts within the IoT category. If you have a novel idea, it is still worth asking the question of its patentability, even if it relates to software. As with many steps in growing a business, securing patent protection is a long-term investment. The journey may be challenging, but the rewards can be equally generous.

Secrecy Ain't Easy: The Trade Secret Alternative

If patent protection is unavailable or unattractive, then another potential option is protecting an invention as a trade secret. This has its own challenges, and not every invention can even possibly qualify as a trade secret. It also bears mentioning that choosing to initiate the patent process

over your invention will quickly eliminate the possibility of trade secret protection.[1] That said, trade secret protection has still been a valuable tool to generate value for growing IoT companies.

First, the definition of a trade secret is quite broad. The Uniform Trade Secrets Act (UTSA), adopted by most states, defines a "Trade Secret" as including "a formula, compilation, program, device, method, technique, or process, that (i) derives independent economic value . . . from not being generally known to, [or] readily ascertainable by . . . other people who can obtain economic value from its disclosure or use, and (ii) is subject of efforts that are reasonable under the circumstances to maintain its secrecy." Some states have adopted an even broader definition. For example, Texas defines a trade secret as encompassing "all forms and types of information, including business, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing . . . ." (See Texas Civil Practice and Remedies Code § 134A.002(6))

Given these sweeping definitions, the largest barrier to trade secret protection is in the name itself: it must be something that can be kept secret, and is kept secret, through reasonable efforts. Thus, the novel and functional physical design of my smart toothbrush might be patentable, but it can never be a trade secret. Everyone who buys the toothbrush can see the design. My revolutionary toothbrush software, however, might be

[1] See, e.g., Accent Packaging, Inc. v. Leggett & Platt, Inc., 707 F.3d 1318, 1329 (Fed. Cir. 2013); Carbo Ceramics, Inc. v. Keefe, 166 F. App'x 714, 719 (5th Cir. 2006); Wellogix, Inc. v. Accenture, L.L.P., 716 F.3d 867, 875 (5th Cir. 2013). (upholding jury instruction explaining that trade secret could not fall within the scope of patent disclosure and collecting cases)

protectable. For example, source code has largely been held protectable as a trade secret.[2] Keep in mind, however, that balanced against that protection is an understanding that anyone can independently write software achieving similar results, which will not violate your "trade secret" rights. Your secret was simply not stolen.

Moreover, as many high school students quickly learn, keeping secrets is sometimes not as easy as you might think. To reasonably protect a secret, everyone with access to the invention, both inside (employees) and outside (investors or partners) an organization must have a legal duty to keep the invention secret. But non-disclosure agreements (NDAs) are not created equal. Simply having employees agree to "not disclose" general information that is shared through the course of a business relationship may not be enough to protect the secret. (See Convolve, Inc. v. Compaq Computer Corp.) In some states, non-competition agreements are simply unenforceable. In California for example, in many instances you cannot restrict an employee from quitting and going to work with your direct competitor, even if that employee is privy to the secret recipe.[3] The employee may still have a duty not to disclose, and the competitor may have a duty not to tease the information out of the employee, but even those duties can be busted by a weak NDA.[4] The truly scary part is that once your agreement is busted, the secret is out, and you've lost your protection. For this reason, companies like Coca-Cola and KFC have notably

[2] See Fitspot Ventures, LLC v. Bier, No. 215CV06454ODWRAO, 2015 WL 5145513, at *3 (C.D. Cal. Sept. 1, 2015) (collecting cases and holding that "Courts have consistently found that source code and customer lists are trade secret information" under California trade secret law.).

[3] C.f. Gatan, Inc. v. Nion Co., No. 15-CV-1862-PJH, 2016 WL 1243477, at *3 (N.D. Cal. Mar. 30, 2016) (although California prohibits non-competition agreements except in cases "necessary to protect its trade secrets", non-compete was invalid because it was not "necessary" to protect company's trade secrets).

[4] See, e.g., Opus Fund Servs. (USA) LLC v. Theorem Fund Servs., LLC, No. 17 C 923, 2017 WL 4340123, at *8 (N.D. Ill. Sept. 29, 2017) (finding non-disclosure agreement unenforceable under Illinois law because it lacked a geographical scope limitation); Kohler Co. v. Kopietzki, No. 13-CV-1170, 2016 WL 1048036, at *2 (E.D. Wis. Mar. 11, 2016) (invalidating non-disclosure agreement restricting disclosure of trade secret "unless and until such confidential information becomes public.")

made secrecy an obsession.[5] Although "keep it secret, keep it safe" may sound like an easy concept, in practice it requires a well-formulated strategy given all of the relationships that a successful company must build.

On the brighter side, consider also that the value in your IoT device and software may lie partially in the data that it collects. Consumer data, such as how often and the length of time I brush my teeth, is arguably a "compilation" of data with independent economic value.[6] Compilations of consumer information, such as emails, purchase history, personal data, and even biometric data have been characterized as assets in capital transactions or even in bankruptcy.[7] Although by no means a settled question, several courts have held that these types of compilations of consumer data could be classified as trade secret assets.[8]

In short, trade secret protection can be a useful and powerful way to protect IoT intellectual property assets. But like with patents, it takes careful planning and strategy. "Secrecy" ain't easy.

Is a Copyright Right for You?

The mere mention of "copyrights" evokes thoughts of the arts, including

[5] Coca-Cola Bottling Co. of Shreveport v. Coca-Cola Co., 107 F.R.D. 288, 294 (D. Del. 1985) (formula locked in a vault); KFC Corp. v. Marion-Kay Co., 620 F. Supp. 1160, 1163 (S.D. Ind. 1985)(no supplier has knowledge of entire seasoning formula)

[6] CHARLENE BROWNLEE & BLAZE D. WALESKI, PRIVACY LAW § 7.08 (2017) ("It is fairly common practice for a business to consider and treat customer lists and the personal information collected from consumers as the property of the business.")

[7] Stacy-Ann Elvy, Commodifying Consumer Data in the Era of the Internet of Things, 59 B.C. L. Rev. 423, 430 (2018) ("If the laws of these states do not apply to a transaction or if other state privacy laws do not clearly cover biometric data, with the possible exception of federal and state unfair and deceptive practices statutes, companies may face few, if any, restrictions on their ability to monetize biometric data.")

[8] See, e.g., Compass iTech, LLC v. eVestment All., LLC, No. 14-81241-CIV, 2016 WL 10519027, at *14 (S.D. Fla. June 24, 2016) (finding that business customer data might be protectable as a trade secret under Florida state law.); PhoneDog v. Kravitz, No. C 11-03474 MEJ, 2011 WL 5415612, at *7 (N.D. Cal. Nov. 8, 2011) (compilation of social media account followers might be protectable as a trade secret)

music, film, books, and paintings. But copyright protects so much more. And major IoT device manufacturers consider copyrights to be a significant part of their IP strategies, especially in a post-Alice/Mayo world.

Copyrights protect "original works of authorship fixed in any tangible medium of expression."[9] Surprisingly for some, this includes software, which copyright law treats as a type of literary work.[10] This does not, however, include "useful articles," in other words, functional things like a toothbrush or charging pod. Although copyright might protect certain artistic features incorporated into a design, such as the sleek look of my smart toothbrush. (See §§903.1, 924) So while copyright may protect your IoT device software, it will not protect your IoT device itself – another reason to consider, and consider early, relying on more than one type of IP right in your overall IP strategy.

Software copyrights have several advantages over software patents. For one, copyrights last longer: Unlike the 20-year duration of a utility patent or the 15-year duration of a design patent, a copyright generally lasts for the life of the author plus 70 years. (See §302(a)) For another, unlike patent rights, which are nonexistent until the federal government issues a patent (after the IP owner successfully completes a multi-year patent application process), a software copyright will exist the moment the code is written. Federal registration is not required in order to have an enforceable copyright; and, also unlike patents, registration can be sought at any time. A timely copyright registration has substantial benefits, and is relatively cheap

[9] 17 U.S.C. § 102(a); Computer Assocs. v. Altai, 982 F.2d 693, 702 (2d Cir. 1992) (noting that "the literal elements of computer programs, i.e., their source and object codes, are the subject of copyright protection").

[10] Technically, copyright law protects the broader subject matter of "computer programs," which extends to all of the copyrightable expression embodied in the computer program, including, for example, source code, and its resulting screen displays. See, e.g., U.S. Copyright Office, Compendium of U.S. Copyright Office Practices ("Compendium (Third)") § 721.1 (3d ed. 2017); see also 17 U.S.C. 101 (defining "computer program" as "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result").

to get—current filing fees range from $35 to $55 per basic application.[11] The U.S. Copyright Office will even allow applicants to redact any lines of code that include trade secret information, provided that the redactions are not excessive. (See U.S. Copyright Office, Circular 61 at 3, noting that the redacted portions of the code containing trade secret material must be "less than fifty percent of the deposit.")

Registration, although not necessary, has its benefits. First, federal registration allows you to file a lawsuit for infringement. As an added bonus, if you file the registration within five years after publishing the work, the facts provided in your copyright application, and the copyright itself, are presumed valid in any litigation. (See § 410(c)) That means the alleged infringer has to prove those facts wrong, and the copyright invalid, rather than the other way around.

Timely registration also affects damages for infringement on the copyright. Copyright infringement remedies include injunctive relief, the destruction of all copies of the infringing work, and the award of actual damages plus a disgorgement of the infringer's profits attributable to the infringement. (See §§502, 503, 504(b)) But delay in filing a registration may limit your damages and eliminate the ability to delay attorneys' fees. In many cases, the ability to recover attorney's fees can significantly impact the decision of whether to enforce your rights in the first place.

But software copyrights are not without their drawbacks. Copyright protection explicitly does not "extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery." (See §102(b)) Rather, copyright protects the expression of those ideas, procedures, et cetera. "As such, the [U.S. Copyright] Office will not register the functional aspects of a computer program, such as the program's algorithm, formatting, functions, logic, system design, or the like . . . , [and]

[11] Bear in mind though that a separate registration is required for every version of your IoT device software that contains new, copyrightable material. See Compendium (Third) at § 721.8.

may refuse registration if the applicant asserts a claim in uncopyrightable elements that may be generated by a computer program, such as menu screens, layout and format, or the like." (See also H.R. Rep. No. 94-1476, at 54 (1976)) In other words, unlike patent protection, copyright law does not prohibit your competitors from creating software that merely functions the same as your IoT device software because copyright law only protects the literal expression of your software's function.

Another limitation is the reality of how software is developed. Copyright does not protect lines of code that are not original; and "originality, as the term is used in copyright, requires both 'independent creation' and 'a modicum of creativity.'"[12] Software is oftentimes written using preexisting code (usually under license from a third party), be it off-the-shelf or open source code. So software oftentimes becomes a compilation of new and preexisting code, which can render the copyright in that software more difficult to enforce because copyright protection belongs to the original author. If you didn't write it, you can't claim copyright protection over that part of the work. (See §103(b))

Software development is also typically a collaborative effort, with lines of code being written by employees, independent contractors, or both. If written by an employee within the scope of employment, then copyright law will treat the employer as the owner of the employee's contributions. (See §201(b)) But if written by an independent contractor, then, absent a signed written agreement to the contrary, the independent contractor might claim ownership or co-ownership of the software copyright—even if you paid good money for the independent contractor's contributions. (See §§201(a)-(b), (d))

To try and overcome some of these challenges, IoT device manufacturers are using their end-user license agreements (EULA) to protect their

[12] Alcatel USA, Inc. v. DGI Techs., Inc., 166 F.3d 772, 787 (5th Cir. 1999) (quoting Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 345 (1991))

copyrights by including language that prohibits certain end-user activities like, for example, reverse-engineering the IoT device's embedded software and modifying or repairing the software. An EULA might even prohibit the resale of an IoT device with its embedded software. For instance, John Deere made headlines a few years ago when the EULA for its software-enabled tractors was criticized for allowing only John Deere and its authorized dealers to repair the on-board software—farmers were not allowed to make the repairs themselves. (See U.S. Copyright Office, Software-Enabled Consumer Products: A Report of the Register of Copyrights 33 n.179 (Dec. 2016), citing news articles from 2015 and 2016.) Despite consumer criticism, the practice—a natural progression of what manufacturers have done for years through their original equipment manufacturer (OEM) software licenses—is likely to expand and continue.[13] Only time and the particulars of each case will tell whether these practices will net enforceable EULA provisions.[14]

IoT device manufacturers might also use digital rights management (DRM) technologies and copyright management information (CMI) to not only limit access to their IoT software and provide notice of their copyright ownership claims, respectively, but to also take advantage of protection provisions in the Digital Millennium Copyright Act, which was passed in 1998, specifically designed to protect electronic works. (See 17 U.S.C. §§1201, 1202) Among other things, these provisions prevent breaches to DRM technologies that you might employ to protect your copyrighted software (e.g., bypassing a digital lock), or the unauthorized removal or alteration of CMI in a copyrighted work.

[13] See U.S. Copyright Office, Software-Enabled Consumer Products 62 ("Although, as noted, the practice of requiring purchasers of software-enabled consumer products to agree to certain written license terms is not uniform today, it is fair to expect that it will increase in the future.").

[14] In a 2016 report, for example, the Register of Copyrights noted that "[t]raditional copyright doctrines such as the idea/expression dichotomy, merger, scènes à faire, and fair use [might] provide a combined and reasonable defense for many tinkering and repair activities," U.S. Copyright Office, Software-Enabled Consumer Products at 33, and that "there have been efforts at the state level to enact 'right to repair' statutes," id. at 33 n.179.

At the end of the day, a software copyright is another tool in the IP toolkit of an IoT device manufacturer. But it is a powerful tool that is relatively easy (and inexpensive) to secure and maintain.

Is Your Idea Worth Protecting?

In short, most definitely. There are many options for protecting IoT intellectual property. Some may be right for your business and others not so much. In any case, the common theme is that IP protection needs an early strategy, especially in the IoT context. The market is growing exponentially, it is highly competitive and the space is ripe for a variety of shenanigans. Without diligence, your dreams of becoming the leader of a smart toothbrush revolution may end up down the drain.

Matt C. Acosta is an intellectual property litigator and advisor experienced in a variety of intellectual property matters. Matt advises clients on a variety of commercial issues, including effective management of e-discovery costs, developing practical expert witness strategies, and navigating the practices of Federal Courts. Though based in Texas, Matt has litigated intellectual property cases throughout the country and has argued before the Judicial Panel on Multi-District Litigation. He has represented and advised a variety of clients, including Fortune 500 companies, in the consumer electronics, biomedical, internet service, mobile application, and telecommunication technology spaces. Matt is a founding member of Jackson Walker's Artificial Intelligence and Blockchain practice groups. He also advises clients and has written a number of articles relating to the emerging Internet of Things.

Entertainment and intellectual property law partner Emilio B. Nicolas is an experienced content and information attorney. His practice includes entertainment, media, technology, and intellectual property litigation and transactional work, with a particular emphasis on copyright, trademark, and privacy law. When Emilio is not advocating for his clients and their intellectual property and business rights in court, he is representing and counseling his clients on intellectual property and media rights management, clearance, and licensing matters, entertainment and media industry transactions, and internet privacy and compliance matters.