FEBRUARY 2019

DEVOTED TO LEADERS IN THE INTELLECTUAL PROPERTY AND ENTERTAINMENT COMMUNITY

VOLUME 39 • NUMBER 2

THE Licensing Journal

Edited by Gregory J. Battersby and Charles W. Grimes

Wolters Kluwer

Don't Lose Your Licensable IP, NDAS and Zero Knowledge Proofs

Yan Song and Adam L.K. Philipp

Adam L.K. Philipp is the founder of AEON Law and head of the firm's patent department. He also counsels clients on intellectual property portfolio strategies and infringement matters.

Yan Song is an IP attorney at AEON Law. She has a Juris Master from Tsinghua University and an LL.M. from the University of Washington, both focused on IP law and policy.

Introduction

It is widely accepted that IP constitutes some of the most valuable assets a company retains.[1] IP holders, therefore, feel the necessity for a guarantee their valuable property is secured effectively.[2] Licensing is one technique where companies can monetize their IP while still preserving their assets. Through strategic licensing, IP assets can be used to greet competitors[3] instead of scaring them away.

One function of IP rights is to encourage the dissemination of new ideas.[4] Even when it comes to trade secrets, by granting certain rights to secret holders and forming a contractual relationship, disclosure of such information becomes voluntary and can lead to the commercialization of the idea.[5] IP licensing encourages this function *via* the well-known nondisclosure agreement (NDA). Some, however, are reluctant to enter into a contract without knowing what they might be limiting themselves from using.[6] It is also not fair for the secret holder to reveal the content of the secret without adequate remedies once the secret is disclosed. This dilemma challenges the functions of a traditional NDA.

Zero Knowledge Proofs (ZKP) are ways to prove something to someone without revealing any of the information that goes into the proofs.[7] Application of this method on Blockchain assures the existence of secrets but their content remains hidden. This technology complements disadvantages of a traditional NDA.

This article will explain the benefits of the NDA for IP licensing and its flaws in terms of licensees' reluctance of entering to an NDA without knowing the authenticity of the secrets and the postponing of redemption of loss. The article will introduce how ZKPs are applied to licensing negotiations to address issues with NDAs and licensing.

IP Licensing and NDAs

Someone may consider a license simply as a permission to use a new technology[8], this is incorrect. Licensing is not permission to use the IP; rather, it is an agreement by the licensor they will not enforce their rights of exclusion against the licensee. A licensee is still an infringer, but they have the license as a defense for their infringing activities.

During licensing negotiations, companies often disclose information containing trade secrets. The best protection for that information is with a nondisclosure agreement.[9] In this chapter, we will introduce the benefits of an NDA for IP licensing with a case study. We will also show the purpose, scope, duration, and specificity of an NDA. (The disadvantage of an NDA will be discussed afterward.)

1. NDA Is Insurance for IP Licensing—*ZeniMax Media, Inc. v. Oculus VR, LLC*

a. NDA and IP Licensing

When an IP owner decides to exploit their IP rights, the owner will often enter into a license agreement with the third-party licensees to make their IP rights available to be used by unaffiliated third parties.[10] By coming together without completely merging, business entities collaborate and work on projects together by sharing IP, information, and know-how in more nuanced and deliberate ways *via* licensing.[11] Though many IP owners may not be aware, licensees are in nature their competitors and intentional infringers. By granting a license, the IP owner turns these intentional infringers into legitimate ones because they can no longer sue the infringer for the infringing activities covered by the license agreement. Similarly, by licensing a trade secret, the owner of that secret partially gives up their monopoly over the secret.[12] More

delicately, in the licensing of know-how, the value of it is gone when the technology it encompasses is gained by the experience of others.[13] This needs to draw IP owners' attention because unlike a patent, which is public information, trade secrets, or know-how, during the process of licensing, are not secrets any more to the other party. As I mentioned before, licensees are competitors and intentional infringers. The revelation of trade secrets, know-how, or any confidential information endangers the competitive advantages of IP owners. Moreover, this disclosure is almost inevitable before or during licensing.

A nondisclosure agreement (NDA) is a contract where at least one party agrees to keep some information confidential.[14] Whenever trade secrets are licensed to third parties, provided to suppliers for use during the manufacturing process, or disclosed to joint venture partners and potential acquirers or investors,[15] an NDA is useful. It is surprising to see that many IP owners overlook the necessity of an NDA, or feel the need but may simply download a template of a generic NDA from the Internet without carefully revising it for IP licensing. We hope the following case *ZeniMax Media, Inc. v. Oculus VR, LLC*[16] may bring attention to the indispensability of an NDA.

b. Case Study: ZeniMax Media, Inc. v. Oculus VR, LLC

Briefly, the plaintiff ZeniMax is a company who developed a virtual-reality (VR) headset but faced the difficulty in overcoming the latency effect, the delay between a user's movement and the corresponding change in the displayed image.[17] One of the defendants, Luckey, is a company who developed a prototype VR headset called the Rift. An employee of ZeniMax, John Carmack, ran into the Rift while browsing an Internet forum. He asked for the Rift prototype from Luckey, modified the Rift, and developed software that reduced latency and prevented image distortions.[18] This breakthrough joined ZeniMax and Luckey to form a formal agreement to protect the incorporated technology in the Rift. With an NDA, Luckey agreed to keep and secure ZeniMax's proprietary information strictly confidential[19] and confirmed that the information was the exclusive property of ZeniMax.

Luckey founded Oculus LLC, raising funds by promoting the Rift. As a response, ZeniMax proposed the two parties to enter into a formal agreement and asked for compensations, but in vain. However, ZeniMax continued feeding Luckey confidential information for unknown reasons. After a few requests by ZeniMax, the two companies finally sat down to discuss future relationship including a license to ZeniMax's VR technology that had been disclosed pursuant to the NDA.[20] An agreement was never reached, and Carmack and a few employees left ZeniMax to join Oculus. Facebook later acquired Oculus. ZeniMax then sued for misappropriation of trade secrets, copyright infringement, and trademark infringement. Though the jury did not find misappropriation of trade secrets, the jury did award the plaintiff with $200 million for actual damages caused by the defendants' breach of the NDA.[21]

We do not need to emphasize more the value of an NDA, specifically in this case, which is worth $200 million. We are obliged to point it out that the NDA in this case not only bound Luckey, but Oculus, which was in fact not the signing party of the NDA. The Court found that Luckey formed Oculus shortly after signing the NDA, and Oculus' purpose was the same as Luckey's to commercialize the Rift.[22] As a founder of Oculus, Luckey was one of its officers, directors, or stockholders.[23] The Court also found that even though Oculus was not a party to the NDA, Oculus requested, received, used, and benefited from confidential information only available to it under the NDA.[24] Under a mere continuation theory[25] and the doctrine of estoppel,[26] the Court decided that Oculus was bound by the NDA as well.

The plaintiff may not predict at the moment of signing the NDA that this agreement will carry such a huge responsibility afterward. They did not even define the purpose of the NDA during the whole time.[27] Though this NDA was not perfect, breach of it incur serious consequences.

2. What Did You Need to Know about Licensing NDAs

a. Types of NDA

There are various types of NDA which protect individuals and businesses, including unilateral agreements, mutual agreements, and NNN agreements.[28]

i. Unilateral Nondisclosure Agreement

A unilateral nondisclosure agreement is appropriate when disclosures will be made by only one of the parties.[29] The receiving party's obligations relating to disclosure and use of the information are the most important provisions.[30] The agreement may also include restrictions on the ability of the receiving party to solicit employees or business partners of the disclosing party.[31] When hiring new employees, employers may use a unilateral NDA.[32]

ii. Mutual Nondisclosure Agreement

A mutual nondisclosure agreement should be used whenever both parties will exchange confidential

information.[33] When two small companies decide to share their own confidential information, a mutual NDA is most often used.[34] If the exchange of confidential information takes place consistently, companies involved can create a model form that permits easy customization to incorporate specific descriptions of the nature and subject matter of disclosures in a particular relationship.[35]

iii. NNN Agreement

The NNN agreement or Non-use, Non-disclosure, and Non-circumvention agreement, is an agreement one needs to deal with the specifics of OEM manufacturing in China.[36] It is a bilingual agreement that protects confidentiality and prevents a Chinese counterpart from competing with a startup or going around the startup by working directly with their customers.[37]

Briefly, "Non-use" prevents Chinese factories from using an idea or concept or product in a way that competes with the IP owner; "Non-disclosure" protects secrets from being spread publicly; "Non-circumvention" bars Chinese factories from selling products at a cheaper price.[38] This agreement can be replaced by a well-drafted Product Manufacturing Agreement if necessary provisions regarding confidential information are included, but before choosing the specific Chinese manufacturer,[39] an NNN agreement is needed to protect one's IP in China.

b. Mutual IP NDA as A Fair Option

The point of the NDA is as a stop-loss if the licensing effort fails. Therefore, it should be made to seem as equitable as possible to encourage signing by the other party. Generally, a mutual NDA will be received more readily than a unilateral NDA. It is not always easy to reach an NDA with the other party, especially when the other party is a big company. For licensors, a mutual IP NDA is useful when your licensees do not want to sign an NDA. By binding both the licensor and their licensees with obligations, this may be perceived as the fairest option for both sides while preserving IP rights.

A mutual IP NDA should include a targeted purpose, the correct scope, proper durations, and special clauses mutually agreed upon by both parties.

i. Targeted Purpose

The purpose of the disclosure and how the information can be used should be specified. For example: "The parties wish to explore a business opportunity of mutual interest and in connection with the financing of one or more potential sale-license-back opportunities, each party may disclose to the other certain confidential technical and business information which the disclosing party desires the receiving party to treat as confidential".[40] Here, the purpose is to explore a business opportunity.

ii. Correct Scope

The scope of the disclosures can be defined in terms of the purpose of the disclosures and the information that will be exchanged,[41] as well as a list of exceptions to ensure that the burdens on the parties are not unreasonable.[42] Provisions like "Recipient shall not have liability to Discloser with regard to any Confidential Information that the Recipient can prove…"[43] can be added to the NDA to distinguish protected information from information in the public domain, unrestricted information, or the information that the Recipient already knew before the disclosure.

iii. Durations

The term of an NDA can be a specific duration of time or under certain conditions. For example, "the foregoing commitments of each party shall survive any termination of the Relationship between the parties, and shall continue for a period terminating five years from the date on which Confidential Information is last disclosed under this Agreement".[44] Here, the duration of the NDA is a five-year commitment.

Another example is "the obligations of each receiving party hereunder shall survive until such time as all Confidential Information of the other party disclosed hereunder becomes publicly known…".[45] The term of this NDA is a condition that if the information is known to the public, the receiving party is released from their contractual obligations.

Usually, as long as the information remains as trade secrets, the NDA lasts; for other confidential information, parties may agree to be bound by the NDA from two to five years.

iv. Special Clauses

A general NDA might not include special clauses, but they can be necessary for certain industries. Reverse engineering, for example, is generally a lawful way to acquire know-how about manufactured products.[46] It is also recognized that the owner of a trade secret does not have an exclusive right to possession or use of the secret information, the protection of which is available only against a wrongful acquisition.[47] Reverse engineering is not a wrongful acquisition; instead, it is deemed as an essential part of innovation.[48] To prevent licensees from reverse-engineering products, a clause prohibiting no reverse engineering can be added so that, although they have

the legal right to do so, they are forbidden based on the NDA.

A residual right clause is another special type worth noting. "Residual" means the retained mental impressions from exposure to trade secrets under an agreement, including ideas, concepts, methods, and techniques disclosed or learned in connection with the trade secret.[49] Ownership of a trade secret encompasses possessions of the residual rights of control over that trade secret.[50] A licensor may prevent a licensee's employees with residual knowledge from working for competitors at least during the agreement[51] because the proof of using residual knowledge is complicated,[52] so clauses like this make it clear cut.

3. What an NDA Cannot Do

NDAs are crucial in many situations, but there are some things an NDA cannot do. As previously mentioned, people are reluctant to enter into NDAs without knowing what they might be limiting themselves from using.[53] Licensees often need solid proof that licensors actually own the trade secret or know-how; however, disclosure of confidential information as such before signing the NDA is unrealistic and also unfair to licensors. Therefore, though an NDA is a useful tool of protecting IP before licensing, asking licensees to enter an NDA may be difficult.

Moreover, cases like *ZeniMax Media, Inc. v. Oculus VR, LLC* are inspiring in that an NDA may be worth millions of dollars once the other party breaches it, but the process of redeeming loss is strenuous and time-consuming. Lawsuits will last for years (*e.g.*, *Oculus* lasted for almost four years). Though compensations can be huge, the time and cash in investment needed is as well.

Due to the two main problems, namely, licensees' reluctance of entering to an NDA without knowing the authenticity of the secrets and the postponing of redemption of loss, an NDA may not protect IP very well under some circumstances. In the next section, we will introduce a complemented method to protect IP prior to licensing.

ZKP and IP Protection

As mentioned previously, licensees are unwilling to enter into an NDA without knowing the authenticity or the content of the confidential information, but it is impractical to require licensors to reveal their secrets before signing the NDA. One solution to this dilemma is the possession of a licensor's secrets is proved to be true. Zero Knowledge Proof (ZKP) systems, are an algorithmic way to prove something to someone without revealing any of the information that goes into that proof.[54] The verifier of the knowledge needs only to be proved with the fact that the prover possesses the secret information[55] instead of the secret information itself. Applying this method to blockchain, licensors, as the provers, can place proof that they possess the confidential information on a blockchain, while the licensees, as the verifiers will be able to prove to their satisfaction that the licensors' possession of the confidential information is true. Moreover, with this proof, licensors have the rationale and power to demand a contemporaneous payment from licensees.

1. The Ali Baba Cave[56]—What is a Zero-Knowledge Proof?

A short story will help to illustrate a simple ZKP: a thief steals Ali Baba's purse and runs into a cave. This cave has two passages, each leading to a dead end. Ali Baba chases after the thief to the left passage but reaches a dead end without encountering the thief. Ali Baba things maybe the thief ran into the right passage. The same incident happens again. Ali Baba chased after the thief, still to the cave, but this time, Ali Baba choses to run into the right passage. No thief is there. The same incident keeps happening to poor Ali Baba, 40 times in a row. Every time Ali Baba is not able to catch the mysterious thief. Then one day, Ali Baba decides to hide in the cave to discover the reasons of why he lost the thief everytime. Surprisingly, Ali Baba hears the thief murmuring a magic word and the dead end opens, the two passages joining together following the incantation.

Many generations later, a young man claims that he knows the secret of the cave. Without revealing the incantation, he asked people to stand outside the cave. He then entered the cave, waiting for the instructions from people outside. They may tell him to come out of the cave from either right or left passage, and he should do accordingly. If he cannot, people would know that he is lying. The young man comes out of the cave every time through the correct passage. Though he does not tell people what the secret is, he proves that he knows the secret. This is called Zero-Knowledge Proof (ZKP).

One may wonder why in the story, people are convinced that the young man indeed possessed the secret? This is a mathematical problem. For the first time, the young man has a 50 percent chance of success guessing which passage people outside may choose to ask him to exit. If this test, however, is repeated 10 times, the percentage of failure will be a cumulative 99.9%. Conspicuously, the young man has to know the secrets to defeat the extremely high

probability of failure in order to succeed every time, which means the fact that he knows the secret is therefore proved to be true.

This story shows an example of an interactive ZKP, which requires interaction between the individual (or computer system) proving their knowledge and the individual validating the proof.[57] In contrast, the noninteractive ZKP (NIZK) is a proof construction where one can prove possession of certain information without revealing that information and without any interaction between the prover and verifier.[58] Applying ZKPs to blockchain, then using blockchain technology to preserve confidential information, one need not disclose the information but others are convinced that the information is true.

2. Zcash and zk-SKNARKs

zk-SKNARK stands for Zero-Knowledge Succinct Non-interactive Argument of Knowledge,[59] a succinct NIZK, having short proofs and fast verification times.[60] Zk-SNARK satisfies four features: completeness, soundness, perfect zero knowledge, and succinctness.[61] Specifically,[62]

1. Completeness: if the statement is true, the verifier will be convinced of this fact by a prover;
2. Soundness: if the statement is false, no cheating prover can convince the verifier that it is true;
3. Perfect ZKP: if the statement is true, no verifier learns anything other than the fact that the statement is true;
4. Succinctness: short proofs and fast verification times.[63]

Theoretically, zk-SNARK can be used to verify any relation without disclosing inputs or leaking information.[64] Zcash is a ZKP blockchain system using zk-SNARKs, allowing senders and receivers of shielded transactions to prove that encrypted transactions are valid.[65] This application mainly focuses on cryptocurrency exchange now, but it is upgrading, and hopefully it will be usable in IP licensing.

3. What Blockchain Can Do

We have introduced ZKP, NIZK, zk-SNARK, and Zcash, depicted features of cutting-edge blockchain technology, and envisioned that it can be used in IP licensing. An NDA, as explained previously, has two flaws: licensees' reluctance of entering to an NDA without knowing the authenticity of the secrets and the postponing of redemption of loss. Zcash allows one to prove possession of certain information without revealing that information.[66] With this feature, licensees are assured that confidential information or trade secrets exist, or the statement regarding this information is true. Therefore, the first flaw of an NDA is cured.

An NDA offers a remedy for breach of contract in that, on one hand, huge damages may be awarded by the Court. On the other hand, though, using an NDA to acquire compensations will be an elongated journey for the infringed party. Fortuitously, with the application of ZKPs on blockchain, compensations may be transferred from the end to the beginning of the licensing negotiations because licensors have the leverage to be paid in advance. This leverage results from the fact that licensors are able to prove with ZKP that statements regarding trade secrets are true. Under a traditional NDA, licensees are not guaranteed with this fact so that negotiations have to happen after signing the NDA. Licensors, therefore, have no grounds to require licensees to pay at this stage. In contrast, proof with ZKP enables licensors to demand a payment in advance respecting the value of the truth and authenticity so that even before signing the NDA, or any occurrence of revealing the trade secrets, licensors have been compensated.

Conclusion

Without IP protection, there are no IP rights[67]; without NDAs, there are no secrets. Both licensors and licensees are highly encouraged to enter into an NDA before licensing negotiations. Once one party breaches the NDA and reveals the confidential information, the Court may award the nonbreaching party huge damages. Relying only on an NDA, however, may not be a good idea. A traditional NDA is not able to guarantee the existence or the truth of confidential information. Additionally, seeking remedies for breaching an NDA through lawsuits is time-and energy-consuming. Thanks to the application of ZKP methods to blockchain, secrets that cannot be told are able to be protected without the revelation of the secrets per se. Moreover, this development will cure the two flaws of a traditional NDA by proving the confidential information before the licensing negotiations and enabling a pre-paid payment mechanism.

1. Donald W. Rupert, *Intellectual Property Litigation Strategies, Commercial Litigation Strategies: Leading Lawyers on Case Preparation, Settlement Opportunities, And Best Practices For Client Success*, Aspatore, 2008, at 1, available at 2008 WL 5939923.
2. Chun-Hsien Chen, *Explaining Different Enforcement Rates of Intellectual Property Protection in the United States, Taiwan, and the People's Republic of China*, 10 Tul. J. Tech. & Intell. Prop. 211, 213 (2007).
3. Supra note 1.

4. Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets As IP Rights*, 61 Stan. L. Rev. 311,333 (2008).
5. *Id*, at 337.
6. *Id*.
7. Mike Orcutt, A Mind-Bending Cryptographic Trick Promises to Take Blockchains Mainstream, *https://www.technologyreview.com/s/609448/a-mind-bending-cryptographic-trick-promises-to-take-blockchains-mainstream/* (last visit December 14, 2018).
8. Eric Adler, The Basics of Open Patent Licensing, *http://techcrunch.com/2015/04/23/open-patent-licensing/* (last time visit December 11, 2018).
9. *Protection of trade secrets—Protection in specific situations—Licensing negotiations*, Corp Couns Gd to Protecting Tr Secrets § 2:40, November 2018.
10. Peter M. Gilhuly, Kimberly A. Posin, Ted A. Dillman of Latham & Watkins LLP, *Intellectually Bankrupt?: The Comprehensive Guide to Navigating IP Issues in Chapter 11, 21 Am*. Bankr. Inst. L. Rev. 1, 2 (2013).
11. Beni Surpin, Matthew Karlyn, *Recent Trends in IP Licensing Require Attorneys to Consider New Opportunities for Monetizing Client Innovation*, February, 2016, at 1, available at 2016 WL 1089430.
12. *The Antitrust Aspects of Trade Secrets*, August, 2018, available at 284 Antitrust Counselor NL 1.
13. *Id.*
14. Nichole Opkins, *Nondisclosure Agreement*, Association of Corporate Counsel, *https://www.acc.com/legalresources/quickcounsel/nondisclosure-agreements.cfm?makepdf=1* (last visited December 13, 2018).
15. Alan S. Gutterman, *Written Nondisclosure Agreements*, Business Transactions Solutions § 199:5, December 2018.
16. ZeniMax Media Inc. v. Oculus VR LLC, No. 3:14-CV-1849-K, 2018 WL 3135915 (N.D. Tex. June 27, 2018).
17. ZeniMax Media, Inc. v. Oculus VR, LLC, No. 3:14-CV-01849-P, 2015 WL 11120970 (N.D. Tex. July 27, 2015).
18. *Id*, at 2.
19. *Id*.
20. *Id*.
21. *https://cdn.arstechnica.net/wp-content/uploads/2017/02/occverdict-1.pdf* (last visited December 17, 2018).
22. Supra Note 16, at 6.
23. *Id*.
24. *Id*.
25. *Id*. Under California law, a company may succeed to another entity's rights and obligations if "there is an express or implied agreement of assumption" or "the purchasing corporation is a mere continuation of the seller." available at Ray v. Alad Corp., 560 P.2d 7, 27 (Cal. 1977).
26. *Id*. In Texas, contract liability may be established under the principle of estoppel.
27. Supra note 16, at 5
28. Non-disclosure, non-use, and non-circumvention.
29. Alan S. Gutterman, *General agreements—Unilateral agreement,* 1 Corp Couns Gd to Strategic Alliances § 8:17, December 2018.
30. *Id*.
31. Alan S. Gutterman, *Trade Secret Protection Programs*, 2010 No. 4 Business Counselor Update 2, April 2010.
32. United States v. Suibin Zhang, No. CR-05-00812 RMW, 2012 WL 1932843 (N.D. Cal. May 29, 2012).
33. Supra note 31.
34. Supra note 14.
35. Supra note 31.
36. Steve Dickinson, Dan Harris, & Grace Yang, *China NNN agreement*, *https://www.chinalawblog.com/2016/02/china-nnn-agreements.html* (last visited December 17, 2018).
37. Chris Carr & Dan Harris, *Internet-of-Things Devices, Intellectual Property, Venture Capital, China Manufacturing, and the Art of A Clean Deal: Who Owns What?*, 34 Santa Clara High Tech. L.J. 315, 325 (2018).
38. Supra note 36.
39. Supra note 37.
40. *Mutual nondisclosure agreement—Patent pending*, 1 Eckstrom's Licensing - Forms § 2A:118, October 2018.
41. Supra note 15, at § 200:113.
42. Id.
43. Id.
44. Id.
45. Supra note 37.
46. Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 Yale L.J. 1575, 1582 (2002).
47. Id.
48. Id, at 1583.
49. Danielle M. Conway-Jones, *Technology Transfer Agreements: Licensing Of Trade Secrets And Works In Development*, SM049 ALI-ABA 103, 110 (2006).
50. *Id*.
51. *Id*.
52. *Id*. "In order to discern whether a licensee's actions are trade secret misappropriation or legitimate exercise of residual knowledge, a licensor will have to survey and identify the available knowledge in the industry before, during, and after licensing the trade secret; identify the licensee's capabilities within the industry to practice the secret; and determine what those in the industry knew separate and apart from the trade secret."
53. Supra note 6.
54. Supra note 7.
55. *https://en.wikipedia.org/wiki/zero-knowledge_proof#cite_note-4* (last visited December 22, 2018).
56. Quisquater Jean-Jacques, Myriam, Muriel, Michael Guillou Louis, Marie Annick, Gaid, Anna, Gwenole, Soazig, *How to Explain Zero-Knowledge Protocols to Your Children*, *http://pages.cs.wisc.edu/~mkowalcz/628.pdf* (last visited January 17, 2019).
57. *https://www.expressvpn.com/blog/zero-knowledge-proofs-explained/* (last visit December 22, 2018).
58. *https://z.cash/technology/zksnarks* (last visited December 25, 2018).
59. Eli Ben-Sasson, Alessandro Chiesa, Christina German, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, *Zerocash: Decentralized Anonymous Payments from Bitcoin*, *http://zerocash-project.org/media/pdf/zerocash-oakland2014.pdf* (last visited January 17, 2019).
60. *Id*.
61. *Id*, at 10.
62. Supra note 59.
63. Supra note 65.
64. Supra note 62.
65. *Id*.
66. Supra note 62.
67. Jim Chester, *The Global View: Developing IP Strategies for International Clients*, November 11, at 2, available at 2011 WL 5618042.