1

IP Rights

Wolters Kluwer | BAKER BOTTS

IP Rights Introduction

Intellectual Property (IP) rights should be a top consideration when developing Big Data systems, particularly for drafting Data Usage Agreements and IP Policies. Collection, transmission, processing, storage, distribution, and other related uses of data can all have important IP implications. What rights are in play? Who owns those rights? At what stage of the process? Can and should they be licensed? These and other question should be asked and answered at the outset of, and continually throughout, a Big Data project.

Given the complexity of Big Data projects and transactions, one can easily imagine a scenario in which multiple parties claim an interest in the same data, further highlighting the importance of data ownership rights. For example, in the case of a smart kitchen appliance that collects data from users, a number of different parties might claim to own the data: the user, the manufacturer of the smart appliance, or an app or software developer who processes that data to gain insights. Given the intangible and non-exclusive nature of data, IP rights and data usage agreements can be the most effective tools for establishing and controlling the ownership of data in complex Big Data projects. In some instances, the dispute as to who owns the rights, or the value of the rights or subject data, may not even be readily apparent at the outset, when an agreement is consummated.

There is no generally applicable default answer to the question of who owns the legal title to collected data in the current U.S. regulatory scheme.[1] As a practical matter, the entity that owns the device that recorded the data usually maintains control of the data,[2] though the confines are not always clear. This uncertainty as to the future value of these IP rights and the subject data is in some instances resulting in stalemates in negotiations of data usage agreements, as companies struggle to allocate the risks associated with all of these uncertainties. IP rights and data ownership issues can be critical parts of these negotiations.

This chapter addresses IP rights as they relate to Big Data systems, including patents, trade secrets, and copyrights. For patents, patent-eligibility of Big Data systems is discussed, as well as infringement and damages issues. The section on trade secrets addresses the differences between patent law and trade secret law, and the particular trade secret concerns for Big Data. The copyright section deals with the applicability of copyright protection to data, databases, and other collections of data.

This chapter also includes sections on Open Source Software, defensive patent approaches, and Standard Essential Patents as these topics relate to Big Data.

Finally, the chapter concludes with an overview of IP Policies in the Big Data space, including pros and cons of various policies in the industry.

---

1 *See* Gareth Corfield, *Internet of Things security? Start with who owns the data,* The Register (Sept. 28, 2016), https://www.theregister.co.uk/2016/09/28/cambridge_wireless_iot_event_defence_sig/.

2 David Knight, *Who owns the data from the IoT?,* Network World (Jan. 30, 2017), https://www.networkworld.com/article/3152837/internet-of-things/who-owns-the-data-from-the-iot.html.

Patent Law

PATENT ELIGIBLE BIG DATA SYSTEMS

As discussed in this sub-section, the patent-eligibility of Big Data systems can depend on a host of factors. For example, factors that weigh in favor of patent-eligibility include claiming a specific technological improvement, solving a problem in a technological area, or combining generic components in an unconventional manner. On the other hand, merely collecting, storing, or manipulating data are factors that weigh against patentability. Several instructive cases are summarized below.

TRADING TECHNOLOGIES INTERNATIONAL, INC. V. CQG, INC.

In a non-precedential decision, the Court of Appeals for the Federal Circuit reviewed the patentability of U.S. Patent Nos. 6,772,132 ("the '132 patent") and 6,766,304 ("the '304 patent"), both of which claim a method and system for electronic trading of stocks, bonds, futures, options, and other products with a specifically structured graphical user interface. The system reduces "the time it takes for a trader to place a trade when electronically trading … thus increasing the likelihood that the trade will have orders filled at desirable prices and quantities."[3] The Federal Circuit concluded that the claims were patentable.

Specifically, for "Section 101 purposes, the claimed subject matter is 'directed to a specific improvement to the way computers operate,' for the claimed graphical user interface method imparts a specific functionality to a trading system 'directed to a specific implementation of a solution to a problem in the software arts.'"[4]

TREEHOUSE AVATAR LLC V. VALVE CORP.

The United States District Court for the District of Delaware reviewed the patentability of U.S. Patent No. 8,180,858 ("the '858 patent").[5] The '858 patent disclosed and claimed a method for "collecting data on network users of a computer game in order to customize items available to users" for purchase during game play.[6] This method solved problems relating to network site loyalty by presenting audio and image data to the user indicative of the user's preferences.[7] The district court determined that the claims were patent eligible.

Specifically, under *Alice* step one, the district court concluded that exemplary claim 1 was not directed to an abstract idea because claim 1 as a whole described more than "the pre-Internet business concept of 'tallying'

---

[3] U.S. Patent No. 6,772,132 (issued Aug. 3, 2004).

[4] *Trading Techs. Int'l, Inc. v. CQG, Inc.*, No. 2016-1616, 2017 WL 192716, at *4 (Fed. Cir. Jan. 18, 2017) (internal citations omitted).

[5] *Treehouse Avatar LLC v. Valve Corp.*, 170 F. Supp. 3d 708 (D. Del. 2016).

[6] *Id.* at 706.

[7] *Id.* at 719.

choices applied in a computer setting."[8] Rather, claim 1 was "directed to users selecting and modifying customizable characters (avatars) in real time on CE sites, as well as storing and retrieving such characters within an information network," which is a series of steps designed to solve a problem related to "network site loyalty."[9] The district court concluded that even if the claims recited an abstract idea, claim 1 was more similar to the claims in *DDR*. The district court reasoned that claim 1 was rooted in computer technology to solve the computer network problem of "network site loyalty" and did not recite a routine or conventional use of a computer.[10] Therefore, the district court concluded that, even if claim 1 was directed to an abstract idea, claim 1 recited an inventive concept and was directed to patentable subject matter.[11]

AMDOCS (ISRAEL) LIMITED V. OPENET TELECOM, INC.

The Federal Circuit reviewed, amongst other patents, U.S. Patent No. 6,418,467 ("the '467 patent). Claim 1 of the '467 patent is directed to a "system, method, and computer program for merging data in a network-based filtering and aggregating platform as well as a related apparatus for enhancing networking accounting data records."[12] The Federal Circuit determined that claim 1 is patent eligible.

Specifically, the Federal Circuit determined even though claim 1 is directed to an abstract idea, claim 1 recites an inventive concept. The court reasoned that claim 1 entails "an unconventional technological solution (enhancing data in a distributed fashion) to a technological problem (massive record flows which previously required massive databases). The solution requires arguably generic components, including network devices and 'gatherers' which 'gather' information. However, the claim's enhancing limitation necessarily requires that these generic components operate in an unconventional manner to achieve an improvement in computer functionality."[13] The court further reasoned that claim 1 was "tied to a specific structure of various components (network devices, gatherers, ISMs, a central event manager, a central database, a user interface server, and terminals or clients). It is narrowly drawn to not preempt any and all generic enhancement of data in a similar system, and does not merely combine the components in a generic manner, but instead purposefully arranges the components in a distributed architecture to achieve a technological solution to a technological problem specific to computer networks."[14] For these reasons, claim 1 was directed to patent eligible subject matter.

CONTEXT EXTRACTION & TRANSMISSION LLC V. WELLS FARGO BANK, ASSOCIATION

The Federal Circuit reviewed the patentability of U.S. Patent No. 5,258,855 ("the '855 patent"). The claims of the '855 patent generally recite a method of "(1) extracting data from hard copy documents using an automated digitizing unit such as a scanner, 2) recognizing specific information from the extracted data, and 3) storing that

---

[8] *See Treehouse Avatar*, 170 F. Supp. at 721.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *See Amdocs (Israel) Limited v. Openet Telecom, Inc.*, 841 F.3d 1288, 1291 (Fed. Cir. 2016).
[13] *Id.* at 1300-01.
[14] *Id.* at 1301.

information in a memory."[15] This method is generally utilized for depositing checks with an ATM.[16] The Federal Circuit concluded that the claims of the '855 patent are invalid.

Specifically, under *Alice* step one, the court concluded that the claims were directed to the abstract idea of (1) collecting data, (2) recognizing certain data within the collected data set, and (3) storing that recognized data in memory, to which the acts of collecting, recognizing, and storing are all well-known in the art.[17] In regards to *Alice* step 2, the court determined that the claims merely recited the use of "existing scanning and processing technology to recognize and store data," that perform "well-understood, routine, and conventional activities commonly used in industry."[18] Furthermore, the court noted that despite the fact that the claims were limited to a particular technological environment (*i.e.*, recognizing and storing information using a scanner or computer), such a limitation was insufficient to transform an abstract idea into a patent eligible subject matter.[19]

CG TECHNOLOGY DEVELOPMENT, LLC V. BIG FISH GAMES, INC.

The United States District Court for the District of Nevada reviewed the patentability of U.S. Patent No. 8,342,924 ("the '924 patent). The '924 patent is directed to an apparatus having processors configured to collect game data, generate statistics based on collected game data, and electronically display the statistics.[20] The district court determined that the claims of the '924 patent are patent ineligible.

Specifically, under *Alice* step one, the district court concluded that the claims are directed to the abstract idea of displaying statistics based on a user's gaming activities and analogized the claims to a method of organizing human activity.[21] Under *Alice* step 2, the district court concluded that the claims do not contain an inventive concept to transform the abstract idea into a patent eligible application because the "technology involved simply carries out the tasks of collecting data from a user's gaming activities and then using the data to generate and display statistics. As with the claims at issue in *Alice*, 'each step does no more than require a generic computer to perform generic computer functions.'"[22]

DIVIDED INFRINGEMENT

There is a risk that the actions of multiple parties may be needed to infringe patents in the Big Data space, and as such, divided infringement may be particularly relevant for companies involved in Big Data. An actor is generally liable for direct infringement when the actor performs every step of a claimed method.[23] However, when the steps of a claimed method are performed by two or more actors, liability can still be found under the doctrine of

---

[15] *See Context Extraction & Transmission LLC v. Wells Fargo Bank, Ass'n*, 776 F.3d 1343, 1345 (Fed. Cir. 2014).
[16] *Id.*
[17] *Id.* at 1347.
[18] *Id.* at 1348.
[19] *Id.*
[20] *See CG Tech. Dev., LLC v. Big Fish Games, Inc.*, No. 2:16-CV-00857-RCJ-VCF, 2016 WL 4521682, at *3 (D. Nev. Aug. 29, 2016).
[21] *Id.* at *3-4.
[22] *Id.* at *4 (citing *Alice Corp. Pty. Ltd. v. CLS Bank International*, 134 S.Ct 2347 (2014).
[23] *Akamai Techs., Inc. v. Limelight Networks, Inc.*, 797 F.3d 1020, 1022 (Fed. Cir. 2015).

divided infringement under 35 U.S.C. § 271(a).[24] Under this doctrine, an actor may be liable for the conduct of others. In the Big Data context this may arise, because often multiple entities are involved in managing or manipulating data. For example, imagine "a smart home solution provider [that] provides to home integrators a smart utility management system including utility meters and sensors to measure temperature and other home environment conditions. The smart utility management system sends data obtained from the utility meters and sensors to the remote cloud storages. The gathered data are used in a Big Data analysis for some useful statistics. The home owners agree to the data gathering [and] will receive some discounts for utility usages."[25] If the described method is patented, the smart home solution provider, the home integrators, and even the home owner could be liable under a theory of divided infringement. Several instructive cases on divided infringement are summarized below.

AKAMAI TECHNOLOGIES, INC. V. LIMELIGHT NETWORKS, INC.

The Federal Circuit broadened the circumstances in which others' acts may be attributed to an accused infringer in cases of divided infringement. An alleged infringer may be held responsible for another's conduct when that conduct is "attributable" to the infringer, i.e., when the infringer "directs or controls" the other party's conduct.[26] The Federal Circuit established a two-part test for analyzing divided infringement. Specifically, liability is appropriate if the alleged infringer "[1] conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and [2] establishes the manner and timing of that performance."[27]

The Federal Circuit also held that members of a joint enterprise may similarly be liable for direct infringement when all the claimed method steps are performed by the members of the joint enterprise. A joint enterprise requires four elements: "(1) an agreement, express or implied, among the members of the group; (2) a common purpose to be carried out by the group; (3) a community of pecuniary interest in that purpose, among the members; and (4) an equal right to a voice in the direction of the enterprise, which gives an equal right of control."[28]

MEDGRAPH, INC. V. MEDTRONIC, INC., 843 F.3D 942 (FED. CIR. 2015)

Without evidence to suggest an agency or contractual relationship, the Federal Circuit evaluated the facts under the Akamai two-prong standard.[29] First, Medgraph failed to prove that Medtronic required the performance of certain method steps by patients and healthcare professionals.[30] Patients were not denied the use of Medtronic's

---

[24] *Akamai Techs., Inc v. Limelight Networks, Inc.*, 786 F.3d 899, 908-09 (Fed. Cir. 2015).

[25] Alex G. Lee, *IoT Business Implications of Joint Infringement*, LinkedIn (August 14, 2015), https://www.linkedin.com/pulse/iot-business-implications-joint-infringement-akamai-v-alex-g-/.

[26] *Limelight Networks*, 786 F.3d at 1022.

[27] *Id.* at 1023.

[28] *Id.* For a further and more recent Federal Circuit discussion of these issues, see *Travel Sentry, Inc. v. David A. Tropp*, No. 16-2386 (Fed. Cir. Dec. 17, 2017) (holding that a party can directly infringe when it benefits vicariously from a third party's infringing acts and has the right and ability to stop or limit the third party's performance of those acts).

[29] *Medgraph, Inc. v. Medtronic, Inc.*, 843 F.3d 942, 947-49 (Fed. Cir. 2015).

[30] *Id.* at 948.

system if they failed to perform steps of the claimed method and Medtronic did not offer incentives to encourage patient performance. Second, Medtronic gave patients latitude regarding when and how to provide their blood glucose data. For example, patients could print or email health data reports for their healthcare professional, or even bring their medical device to a provider to have the blood sugar data extracted. Accordingly, Medtronic did not exercise control of the timing or manner of their patients' performance.[31] With neither Akamai prong satisfied, the Federal Circuit affirmed summary judgment of non-infringement.[32]

VALUATION AND DAMAGES

VIRNETX, INC. V. CISCO SYSTEMS, INC.

It is generally preferable to pursue a theory of direct infringement when possible, as, amongst other things, the proofs required can be more straightforward, and damages awards may be impacted when infringement is proven under a theory of divided infringement. Specifically, "[w]hen patent claims are drawn to an individual component of a multi-component product, it is the exception, not the rule, that damages may be based upon the value of the multi-component product."[33] In *VirnetX*, the Federal Circuit established that in divided infringement cases, the plaintiff will sometimes be limited to a portion of the market value of the accused product, instead of the full value. "Where the smallest salable unit is, in fact, a multi-component product containing several non-infringing features with no relation to the patented feature (as VirnetX claims it was here), the patentee must do more to estimate what portion of the value of that product is attributable to the patented technology."[34]

PATENT EXHAUSTION DOCTRINE

The Patent Exhaustion Doctrine states that "the authorized sale of an article that substantially embodies a patent exhausts the patent holder's rights and prevents the patent holder from invoking patent law to control post sale use of the article."[35] The Supreme Court in *Motion Picture Patents* established that the patent exhaustion doctrine is triggered (1) with an authorized and unconditional sale of the patented article and (2) when the patented article possesses the essential inventive features of the corresponding patent.[36] In the context of Big Data, the patent exhaustion doctrine could arise more frequently with regards to methods or machines designed to manipulate data, since these aspects of a Big Data system are more likely to encompass patent eligible subject matter, as discussed above.[37]

QUANTA COMPUTER, INC. V. LG ELECS., 553 U.S. 617, 629 (2008).

This case illustrates how a method can be subject to patent exhaustion. LG Electronics [hereinafter "LGE"] licensed patents to intel. LGE and Intel entered into an agreement that required Intel to give their customers notice that the agreement did not extend to products made by combining an Intel and non-Intel product. Quanta purchased

---

[31] *Id.*
[32] *Id.* at 948-49.
[33] *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1326 (Fed. Cir. 2014).
[34] *Id.* at 1328-29.
[35] *Quanta Computer, Inc. v. LG Elecs.*, Inc., 553 U.S. 617, 638 (2008).
[36] *Motion Picture Patents Co. v. Universal Film Mfg. Co.*, 243 U.S. 502 (1917).
[37] *See JVC Kenwood Corp. v. Nero, Inc.*, 797 F.3d 1046 (Fed. Cir. 2015).

microprocessors from Intel and made computers for Dell, Hewlett-Packard, and Gateway (in violation of the agreement). LGE sued for infringement.[38] The Supreme Court held that patent rights associated with a method patent are exhausted by the sale of an item that substantially embodies the method.[39] "Because the doctrine of patent exhaustion applies to method patents, and because the License Agreement authorizes the sale of components that substantially embody the patents in suit, the exhaustion doctrine prevents LGE from further asserting its patent rights with respect to the patents substantially embodied by those products."[40]

IMPRESSION PRODUCTS, INC. V. LEXMARK INTERNATIONAL, INC.

The Supreme Court held that a patent owner may not prevent the application of the patent exhaustion doctrine by accompanying post-sale restrictions on the sale of a patented good. "Once a patentee decides to sell—whether on its own or through a licensee-that sale exhausts its patent rights, regardless of any post-sale restrictions the patentee purports to impose, either directly or through a license."[41]

The Supreme Court held that patent exhaustion applies to all sales, even if the sale occurs outside of the United States. "Exhaustion does not depend on whether the patentee receives a premium for selling in the United States, or the type of rights that buyers expect to receive. As a result, restrictions and location are irrelevant; what matters is the patentee's decision to make a sale."[42]

---

[38] *Quanta Computer, Inc. v. LG Elecs.*, Inc., 553 U.S. 617 (2008).
[39] *Id.* at 629.
[40] *Id.* at 617.
[41] *Impression Prods. Inc., v. Lexmark Int'l, Inc.*, 137 S. Ct. 1523, 1536 (2017).
[42] *Id.* at 1538.

Trade Secrets

PURPOSE OF TRADE SECRET LAW

While patents remain a strong form of IP protection—and arguably continue to be, generally speaking, the most valuable—obtaining a patent in the field of Big Data analytics can be difficult in the wake of the Supreme Court's *Alice* decision on patent eligible subject matter.[43] In some cases, trade secret law may offer an easier and more effective means of protecting commercially valuable proprietary information that gives a competitive advantage in the Big Data context, both in connection with algorithms and AI engines and the important and valuable collections of data they generate and process.[44] For example, companies have used trade secret law to protect formulas, manufacturing processes and techniques, business strategies and management information, compilations (*e.g.,* customer lists), and design concepts.[45] In the field of Big Data, trade secret law has also been used to protect the algorithms and analytic techniques used to glean valuable information from data.[46]

DIFFERENCES BETWEEN TRADE SECRET LAW AND PATENT LAW[47]

There are fundamental differences between trade secret law and patent law, including:

- A valid trade secret is protectable for potentially unlimited duration;
- Trade secret law does not come with the jurisdictional limitations associated with U.S. patents;
- Information protected under trade secret law remains undisclosed, and as discussed further below, protection depends on the trade secret holder's efforts to keep the information secret;
- Obtaining and maintaining trade secret protection depends on the owner's actions, whereas in patent law, protection is dependent on both owner and government actions.

TRADE SECRET LEGISLATION

Prior to the passage of the Defend Trade Secrets Act ("DTSA") in 2016, state law provided the sole remedy for trade secret misappropriation. However, with passage of the DTSA, trade secret holders now have a uniform federal cause of action for misappropriation and easier access to federal courts in addition to the rights provided

---

[43] *See Alice Corp. v. CLS Bank Int'l*, 134 S.Ct. 2347 (2014).

[44] *Trade Secret Protection in the U.S.*, USPTO.gov, at 2-3, https://www.nist.gov/sites/default/files/documents/mep/marinaslides.pdf.

[45] *Id.*

[46] *See, e.g.*, Steve Lohr, *Google Schools Its Algorithm*, New York Times (March 5, 2011), http://www.nytimes.com/2011/03/06/weekinreview/06lohr.html ("[Google's] algorithm is a tightly guarded trade secret . . . .").

[47] *Trade Secret Protection in the U.S.*, *supra* note 44, at 12.

by state trade secret laws. [48] The following sections provide a brief overview of trade secret protection under the DTSA and Uniform Trade Secrets Act, which has been largely codified by the states.

UNIFORM TRADE SECRETS ACT (UTSA)

Although the UTSA does not expressly contemplate computer source code as protectable (as the DTSA does below), the definition of a trade secret under the UTSA is expansive and likely protects Big Data.[49] The UTSA was promulgated by the Uniform Law Commission in an effort to harmonize state laws regarding the misappropriation of trade secrets.[50] While state trade secret laws do vary, every state that has passed trade secret legislation has adopted the UTSA, in some form, except for New York and Massachusetts.[51] The following definitions and remedies provided in the UTSA are particularly relevant.

A trade secret is "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[52]

Misappropriation of a trade secret means: "(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who has utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his position, knew or had reason to know that it was a trade secret ad that knowledge of it had been acquired by accident or mistake."[53]

Injunctive relief is available under the UTSA. Specifically, "[a]ctual or threatened misappropriation may be enjoined. Upon application to the court an injunction shall be terminated when the trade secret has ceased to exist, but the injunction may be continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation."[54]

---

[48] Cohen, Ben, et. al., *Explaining the Defend Trade Secrets Act*, AmericanBar.org, https://www.americanbar.org/publications/blt/2016/09/03_cohen.html.

[49] *See A Recipe for New Info Governance and Data Asset Protection,* Kilpatrick Townsend & Stockton LLP (Jan. 7, 2014), http://www.kilpatricktownsend.com/~/media/Files/articles/2014/NEIDITZLAW360.ashx.

[50] Uniform Trade Secrets Act with 1985 Amendments.

[51] Coyne, Patrick J., *What You Should Know About the Defend Trade Secrets Act*, Law360 (Jun. 28, 2016), http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=1444a1c9-e0d0-4e07-afd4-3fd671d2fafc.

[52] Uniform Trade Secret Act § 1(4).

[53] Uniform Trade Secret Act § 1(2).

[54] Uniform Trade Secret Act § 2(a).

Damages are also available under the UTSA, which states that "(a) [e]xcept to the extent that a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation renders a monetary recovery inequitable, a complainant is entitled to recover damages for misappropriation. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret. … (b) If willful and malicious misappropriation exists, the court may award exemplary damages in the amount not exceeding twice any award made under subsection (a)."[55]

DEFEND TRADE SECRETS ACT (DTSA)

The DTSA is particularly relevant to Big Data analytics, because it specifically allows for the protection of computer source code as a trade secret. Trade secret holders may also find the nationwide applicability and access to federal courts afforded by the DTSA preferable to the misappropriation remedies and forums available under state trade secret law. The following definitions and remedies provided in the DTSA are particularly relevant.

A trade secret is "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if the owner thereof has taken reasonable measures to keep such information secret; and the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."[56]

The DTSA defines misappropriation of a trade secret in substantially the same way as the UTSA.

Injunctive relief is available under the DTSA. However, a court may not grant an injunction when the injunction would "prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or (II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."[57]

Additionally, damages are also available for "actual loss caused by the misappropriation of the trade secret" and "for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss."[58] Exemplary damages may be available when the trade secret is "willfully and maliciously misappropriated" in an amount not greater than two times the compensatory damages awards.

---

[55] Uniform Trade Secret Act § 3(a)-(b).
[56] 18 U.S.C. § 1839(3).
[57] 18 U.S.C. § 1836(b)(3)(A)(i)(II).
[58] 18 U.S.C. § 1836(b)(3)(B)(i)(I)-(II).

Under the DTSA, a court may issue an ex parte civil seizure order under 35 U.S.C. § 1836 "providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is subject of the action."[59] Civil seizures will be ordered only in extraordinary circumstances, and before a seizure order can be issued, it must be shown that:

- The relief pursuant to Fed. R. Civ. P. 65, or other equitable relief, would be inadequate;
- an immediate and irreparable injury will occur if seizure is not ordered;
- harm to the applicant of denying the application of a seizure order (1) outweighs the harm to the person against whom seizure is ordered and (2) substantially outweighs the harm to any third parties by such seizure;
- the applicant is likely to succeed in showing that the person against whom the order is issued misappropriated or conspired to misappropriate a trade secret through improper means;
- the person against whom the order will be issued has actual possession of the trade secret and any property to be seized;
- the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, the matter's location;
- the person against whom seizure is ordered would destroy, move, hide, or otherwise make such property inaccessible to the court if put on notice; and
- the applicant has not publicized the requested seizure.[60]

Other particularly relevant elements of the DTSA include:

- Whistleblower Immunity
  - The DTSA provides for whistleblower immunity from both federal and state trade secret misrepresentation actions. That is, an individual faces no criminal or civil liability for "the disclosure of a trade secret that is made [i] in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney … [ii] solely for the purpose of reporting or investigating a suspected violation of law … [or B] in a complaint or other document filed in a lawsuit or other proceeding, if such a filing is made under seal."[61]
- Employer Notification Requirement
  - Employers under the DTSA are required to provide notice of the immunity provisions in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information."[62]

[59] 18 U.S.C. § 1836(b)(2)(A)(i).
[60] 18 U.S.C. § 1836(b)(2)(A)(ii).
[61] 18 U.S.C. § 1833(b)(1)(A), (B).
[62] 18 U.S.C. § 1833(b)(3)(A).

- Protection for Trade Secrets in Court
  - The DTSA seeks to prevent trade secrets from being revealed in court. Specifically, it states that "The court may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential."[63] This framework gives trade secret owners the opportunity to indicate to the court why particular information should remain secret.

FACTORS THAT COURTS CONSIDER TO DETERMINE WHETHER AN ENTITY HAS A PROTECTABLE TRADE SECRET

As discussed above, both the UTSA and DTSA require owners of trade secrets to take reasonable measures to protect the secrecy of the information they seek to protect. Many courts utilize six factors recited in the Restatement of Torts to determine whether an entity has a protectable trade secret. These factors include: "(1) the extent to which the information is known outside of [the] business; (2) the extent to which it is known by employees and others involved in [the] business; (3) the extent of measures taken by [the business] to guard the secrecy of the information; (4) the value of the information to [the business] and [its] competitors; (5) the amount of effort or money expended by [the business] in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others."[64]

The extent of measures taken to guard the secrecy of the information is frequently considered the most important factor when evaluating whether a trade secret is protectable.[65] Importantly, the owner of a trade secret need not keep the information absolutely secret, but rather exercise a reasonable amount of precaution to protect the confidentiality of the trade secret.[66]

WHERE TO PURSUE A TRADE SECRET MISAPPROPRIATION ACTION?

As discussed above, the DTSA created a federal cause of action for trade secret misappropriation, and an entity may pursue a misappropriation remedy in federal court for misappropriation occurring on or after May 11, 2016, assuming additional jurisdictional requirements are met. To qualify for federal jurisdiction, the DTSA mandates that the misappropriation at issue involve a trade secret that "is related to a product or service used in, or intended for use in, interstate or foreign commerce."[67] Trade Secret holders seeking a remedy for misappropriation that occurred prior to May 11, 2016, or which does not meet the additional requirements for federal jurisdiction, can still seek recourse under state law.

---

[63] 18 U.S.C. § 1835(b).

[64] *See Ashland Mgmt. Inc. v. Janien*, 82 N.Y.2d 395, 406 (1993) (citing Restatement of Torts § 757, comment *b*); *see also, e.g.*, *N. Atl. Instruments, Inc. v. Haber*, 188 F.3d 38, 44, 15 I.E.R. Cas. (BNA) 731, 51 U.S.P.Q.2d 1742, 139 Lab. Cas. (CCH) P 58738 (2d Cir. 1999); *In re Bass*, 113 S.W.3d 735, 739, 164 O.G.R. 834 (Tex. 2003); *Wal-Mart Stores, Inc. v. P.O. Market, Inc.*, 347 Ark. 651, 66 S.W.3d 620, 630 (2002); *Combs & Associates, Inc. v. Kennedy*, 147 N.C. App. 362, 555 S.E.2d 634, 640, 18 I.E.R. Cas. (BNA) 263 (2001).

[65] *See Integrated Cash Management Services v. Digital Transactions, Inc.*, 920 F.2d 171, 173 (2nd Cir. 1990).

[66] *§ 14:8. Elements of a claim -- "What is a trade secret? -- "The information must be secret*, Litigating Business and Commercial Tort Cases.

[67] 18 U.S.C. § 1836(b)(1).

COMPARISON BETWEEN DTSA ACTIONS AND UTSA ACTIONS

	UTSA	**DTSA**
Definition of Trade Secret	"Information . . . that: (i) derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." U.T.S.A. § 1(4).	"All forms and types of financial, business, scientific, technical, economic, or engineering information, including . . . programs, or codes . . . if— (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;" 18 U.S.C. § 1839(3).
Definition of Improper Means	Not explicitly defined. Comments indicate that improper means "could include otherwise lawful conduct which is improper under the circumstances . . . ."	"(A) includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means; and (B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition." 18 U.S.C. § 1839(6).
Injunctive Relief	"Actual or threatened misappropriation may be enjoined." U.T.S.A. § 2.	Available "to prevent any actual or threatened misappropriation . . . provided the order does not— (I) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or (II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business;" 18 U.S.C. § 1836(3).
Exemplary Damages and Attorney Fees	Exemplary damages available in cases of willful and malicious misappropriation. Attorney fees available upon showing of bad faith, and in cases of willful and malicious misappropriation. U.T.S.A. §§ 3(b), (4).	Exemplary damages and attorney fees available under same conditions as UTSA. However, in an action by an employer against an employee, exemplary damages and attorney fees may not be awarded if the employer does not comply with the whistleblower immunity notice requirement of 18 U.S.C. § 1833.
Ex parte Civil Seizure	Remedy not available under UTSA.	"[T]he court may, upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action." 18 U.S.C. § 1836.
Choice of Law	State procedural rules vary, and implementation of the UTSA has not been uniform across all 50 states. Traditional choice of law principals apply.	Federal Rules of Civil Procedure apply in federal court. DTSA is a federal statute, which should be applied uniformly nationwide. Traditional choice of law principals may still apply when determining whether an injunction would "conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."

Copyright

COPYRIGHT PROTECTION FOR COLLECTED DATA

In contrast to patents and trade secrets, copyright protection does not allow a rights holder to exclude others from using ideas or information, and as such, raw data itself is not copyrightable.[68] However, an original arrangement or compilation of raw data may be protected under copyright law.[69] According to the U.S. Copyright Office, "[a]n application to register a database typically covers the selection, coordination and/or arrangement of data, information or files, but does not cover the data, information or files unless they are specifically claimed in the application."[70] The EU approach similarly focuses on the arrangement of data, granting copyright protection to databases, "which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation . . . ." As discussed further below, the EU also provides a *sui generis* right "to prevent extraction and/or re-utilization of the whole or of a substantial part . . . " of a database when there has been "substantial investment in obtaining, verifying, or presenting the contents [of the database]. . . ."[71]

Under U.S. copyright law, a copyright owner has the exclusive right to create derivative works based on their copyrighted work.[72] A copyright owner "may claim copyright in a work that recasts, transforms, or adapts a [copyrighted] work."[73] With respect to Big Data, the ownership of derivative works frequently comes into play when databases are shared between parties. "For example, a licensee may license a database and then spend hundreds of hours mining the database for information generating analysis and new sets of data based on the derivative works of such data mining and analysis."[74] As discussed in the following section, the fair use doctrine can create uncertainty regarding the ownership of derivative works, again highlighting the importance of a comprehensive DUA addressing data ownership.

---

[68] *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 344 (1991) ("Facts are not copyrightable.").

[69] *Feist Publ'ns, Inc.*, 499 U.S. at 348 ("[The compilation author's] choices as to selection and arrangement, as long as they are made independently by the compiler and entail a minimal degree of creativity, are sufficiently original that Congress may protect such compilations through the copyright laws."); *Gemel Precision Tool, Co. v. Pharma Tool Corp.*, 1995 WL 71243, at *4 (E.D. Pa. Feb. 13, 1995) ("While it is true that factual information generally accessible to the public is not protected by copyright law, the compilation of those facts may be copyrightable.").

[70] U.S. COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 1002.6 (3d ed. 2014) [hereinafter "COMPENDIUM"].

[71] EU Directive 96/9/EC on the Legal Protection of Databases.

[72] COMPENDIUM § 507.2.

[73] COMPENDIUM § 507.2.

[74] Aaron K. Tantleff, *Licensing Big Data*, *in* BIG DATA: A BUSINESS AND LEGAL GUIDE 91, 95 (James R. Kalyvas & Michael R. Overly eds., 2015).

DERIVATIVE WORKS AND FAIR USE

A copyright exception for transformative derivative works exists under the fair use doctrine.[75] Under the fair use doctrine, a court will look to four factors to determine whether a derivative work constitutes a fair use such that there is no copyright infringement.[76] The factors are "[1] the purpose and character of the use, [2] the nature of the copyrighted work, [3] the amount and substantiality of the portion used in relation to the copyrighted work as a whole, and [4] the effect of the use upon the potential market for or value of the copyrighted work."[77] Under the first factor, "the purpose and character of the use," a court will look to whether the use is transformative, i.e. "altering the original with new expression, meaning, or message."[78]

A key question, therefore, is whether Big Data analysis transforms a dataset. A data licensee may argue that its Big Data analysis alters the original dataset with new meaning so as to transform the dataset.[79] On the other hand, the licensor may argue that the analysis is not so great so as to transform the copyrighted database.[80] In order to avoid such conflicts over the copyrights to the original database and any derived works, IP ownership should be clearly allocated in a DUA, as discussed in Chapter 5 below.

FEIST PUBLICATIONS, INC. V. RURAL TELEPHONE SERVICE COMPANY, INC.

The Supreme Court held that a phonebook containing thousands of names and their telephone numbers was not entitled to copyright protection because the phone book merely included uncopyrightable facts.[81] Furthermore, the facts were not "selected, coordinated, or arranged" in an original way to satisfy the originality prong for obtaining copyright protection because the phone book listed the information in an entirely typical manner and this selection "lack[ed] the modicum of creativity necessary to transform mere selection [of facts] into copyrightable expression."[82]

The court made the following points. "Facts are not copyrightable."[83] However, compilations of facts may satisfy the originality requirement to obtain copyright protection for a work because "[t]he compilation author typically chooses which facts to include, in what order to place them, and how to arrange the collected data so that they may be used effectively by readers. These choices as to selection and arrangement, so long as they are made independently by the compiler and entail a minimal degree of creativity, are sufficiently original that Congress may protect such compilations through the copyright laws."[84] This copyright protection is subject to the limitation that "[t]he mere fact that a work is copyrighted does not mean that every element of the work may be protected.

---

[75] Copyright Act of 1976, 17 U.S.C. § 107.
[76] *Id.*; *see* More Information on Fair Use, COPYRIGHT.GOV, https://www.copyright.gov/fair-use/more-info.html (last visited July 28, 2017).
[77] 17 U.S.C. § 107.
[78] *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 569 (1994).
[79] *See id.*
[80] *See id.*
[81] *See Feist Publications, Inc. v. Rural Telephone Service Company, Inc.*, 499 U.S. 340, 361 (1991).
[82] *Id.* at 361–62.
[83] *Id.* at 344.
[84] *Id.* at 348.

Originality remains the sine qua non of copyright; accordingly, copyright protection may extend only to those components of a work that are original to the author."[85]

This case is instructive in the Big Data context. For example, imagine a retailer collecting and storing the names of its customers unaltered in a database. This is analogous to a phonebook and such a database would likely not be able to receive copyright protection. On the other hand, imagine a retailer conducting an online survey of the age and gender of its users. Next the retailer sorts the results by age, deletes impossible answers, deletes suspected repeat answers, and transforms the resulting data into two graphs for each gender. The resulting database appears more in line with the Supreme Court's "minimal creativity" requirement above, and thus, such a database would be more likely to receive copyright protection.

FIRST SALE DOCTRINE IN COPYRIGHT

The first sale doctrine of copyright law [hereinafter "FSD"] is an old concept, originally described by the Supreme Court in 1908.[86] Now codified in 17 U.S.C. § 109, the FSD refers to how the first sale of a copyrighted work prevents the copyright owner from controlling the distribution or resale of that work.[87] The Supreme Court in *Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519 (2013) held that the FSD also applies to any copyrighted work that is lawfully made and sold abroad.

The FSD has historically been reliable in protecting resellers of copyrightable content. For example, picture a retailer that sells used books, including books printed by a certain publisher. The FSD is the reason the publisher cannot sue the retailer in this hypothetical. In the digital space, the first sale doctrine is less certain. In 2013, the Southern District of New York held that "the first sale defense is limited to material items, like records, that the copyright owner put into the stream of commerce."[88] This decision cast uncertainty over the FSD's application in the digital space, however the Second Circuit's anticipated appellate ruling may clarify the FSD's role.[89]

SUI GENERIS RIGHT IN THE EU

In February of 1996, the European Union adopted Directive 96/9/EC concerning the Legal Protection of Databases.[90] This directive vests a *sui generis* right in the maker of a database that shows "there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents."[91] Specifically, there are three requirements to gain the IP right: 1) the maker of the database is a national of an EU member state or is a company located within the EU community with operations genuinely

---

[85] *Id.*

[86] *Bobbs-Merrill Company v. Straus*, 210 U.S. 339 (1908).

[87] 17 U.S.C. § 109.

[88] *Capitol Records, LLC v. ReDigi Inc.*, 934 F. Supp. 2d 640, 655 (S.D.N.Y. 2013);

[89] Lee Burgunder, *Digital Resale & Copyrights: Why the Second Circuit Won't Buy It,* IP Watchdog (Oct. 11, 2017), http://www.ipwatchdog.com/2017/10/11/digital-resale-copyrights-second-circuit-wont-buy/id=88965/.

[90] *Protection of Databases*, European Commission, http://ec.europa.eu/internal_market/copyright/prot-databases/index_en.htm (last updated Jun. 6, 2016).

[91] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, 2004 O.J. L 77/20, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996L0009&from=EN.

linked with the economy of an EU member state; 2) the maker made a "substantial investment" in obtaining, verifying, or presenting the data; and 3) the data was formed into a database.[92]

In a typical Big Data scenario, where multiple entities interact with the data, recognizing the maker will usually be the most difficult step.[93] "The maker will be the entity who:

- takes the initiative in obtaining, verifying or presenting the contents of the database; and
- assumes the risk of investing in that obtaining, verifying or presenting."[94]

It is important to note that although 96/9/EC vests data rights in an entity that meets these requirements, it does not necessarily exclude entities that fail these requirements. In situations where 96/9/EC is not met, uncertainty remains.

[92] *Who owns the data in the Internet of Things?*, Taylor Wessing (Feb. 2014), https://united-kingdom.taylorwessing.com/download/article_data_lot.html.
[93] *Id.*
[94] *Id.*

Open Source Software

WHAT IS OPEN SOURCE SOFTWARE

Open Source Software ("OSS") is a general term for software with source code that anyone can inspect, modify, and enhance. OSS differs from Proprietary Software ("PS") in that users of PS are unable, either literally or legally, to access the source code of the software.[95] For either OSS or PS, the user must accept the terms of a license when they use the software, but the terms of the licenses differ: OSS licenses generally grant permission to use the software as desired, whereas PS licenses often restrict use and distribution rights.

The term "open source" has been used generically to describe software with varying degrees of proprietary restrictions: some allow completely free modification, some require that any modifications to the software be made available to the public (sometimes called "copy-left" licenses), and others require that sharing those modifications be royalty free (sometimes called "copy-free").[96] The Open Source Initiative, an organization dedicated to evaluating the openness of technology licenses,[97] has attempted to keep the term "Open Source" specific. It has created a list of attributes that any license must have to be added to their list of 'truly' open source licenses.[98]

OSS is being created and used by many different companies for a variety of applications. For example, Google is one of the largest contributors to OSS: during the last decade, it created over 2000 open source projects. Android, Angular, Chromium, and Go are some of the most successful OSS projects from Google.[99] Netflix, Macys, Ford, and others are using OSS to gather, process, and make use of large amounts of data.[100]

---

[95] *What is open source?*, Opensource.com, https://opensource.com/resources/what-open-source (last visited Oct. 31, 2017).

[96] Stephen R. Walli, *Which open source software license should I use?*, Opensource.com (Jan. 29, 2013), https://opensource.com/law/13/1/which-open-source-software-license-should-i-use.

[97] *About the Open Source Initiative*, Opensource.com, https://opensource.org/about (last visited Oct. 31, 2017).

[98] *The Open Source Definition (Annotated)*, Opensource.com, https://opensource.org/osd-annotated (last visited Oct. 31, 2017).

[99] Janakiram MSV, *How Google Turned Open Source Into a Key Differentiator For Its Cloud Platform*, Forbes (Jul. 9, 2017), https://www.forbes.com/sites/janakirammsv/2017/07/09/how-google-turned-open-source-into-a-key-differentiator-for-its-cloud-platform/#403c378f646f.

[100] Scott Gnau, *Open Source Is The New Normal In Data Analytics*, Forbes (Jul. 11, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/07/11/open-source-is-the-new-normal-in-data-and-analytics/2/#475d23bc742a.

APPLICATION TO BIG DATA

Open Source Software can be very useful when dealing with Big Data. OSS can been used to build either cloud computing systems or local computing systems that can process vast amounts of information.[101] For example, some Ford vehicles are capable of generating up to 25 gigabytes of data per hour, and the company uses OSS to collect vehicle data and improve the driving experience in their cars.[102] Netflix collects data about user preferences to suggest programs, Macys collects purchasing data to target marketing, and Progressive Insurance collects driving data to set insurance rates; all using OSS.[103] In 2014, Google created an open source software development kit called Dataflow to process data. It was immediately available as Cloud Dataflow, a managed service in Google Cloud Platform to run data processing pipelines at scale."[104]

OSS is particularly useful for analyzing Big Data because of the ease of compatibility.[105] Managing Big Data requires programs on multiple machines to work together in an efficient way, so that each program knows which components of the data to store locally, which components to process, and how to combine that data for analysis. This requires interactivity and special programming techniques which have already been worked out by OSS contributors.[106]

POTENTIAL CONCERNS

Using OSS can create legal concerns that impact business decisions. These concerns can vary widely depending on the specifics of the licenses involved with the OSS—each OSS source can come with its own specific restrictions—a common restriction being that modifications to OSS must be redistributed into the OSS community.[107] For example, imagine a company that is interested in using a piece of OSS. They would first need to download it and likely would need a programmer of their own to modify the OSS to suit their own needs. Many who successfully preform this modification might want to sell their modified OSS to similarly situated companies, but OSS often comes with a prohibition on this sort of sale. For this reason, companies that modify OSS sometimes charge users money for software services and support rather than for the software itself to generate revenue from their

---

[101] *An introduction to big data*, Opensource.com, https://opensource.com/resources/big-data (last visited Oct. 31, 2017).

[102] Owners can track the location of their cars, check fuel levels, receive diagnostic alerts, and more, all through a phone app. Ford is able to track trends across models to improve warranties and support. Doug Henschen, *Hadoop Summit 2016 Spotlights Enterprise Innovation, IoT Use Cases*, Data to Decisions, https://doughenschen.com/2016/07/01/hadoop-summit-2016-spotlights-enterprise-innovation-iot-use-cases/ (last visited Oct. 31, 2017) [hereinafter "Henschen"].

[103] *See* Henschen, *supra* note 102; Gnau, *supra* note 100.

[104] *See* MSV, *supra* note 99.

[105] *See An introduction to big data*, *supra* note 101.

[106] *Id.*

[107] Scott Nesbitt, *Is making your product free and open source crazy talk?*, Opensource.com (Jul. 14, 2014), https://opensource.com/business/14/7/making-your-product-free-and-open-source-crazy-talk.

software.[108] If the OSS is available for free, using it may present large upfront savings for a company looking to analyze data, however, it may be impossible to prevent competitors from using the customized OSS. The business decision of whether to use OSS as a starting point may rest on whether the data (which cannot be copied even with OSS) or the software that analyzes it (which can) is more valuable.

Copyright implications should also be considered when dealing with OSS. Commonly used OSS licenses often address copyright issues and limit the rights of users by requiring them to license any modifications or derivative works to the public. Ownership of an OSS copyright is sometimes unclear if the creator of the work is not a single person or entity. However, a free licensing requirement is an easy and powerful remedy to this problem. These more restrictive OSS licensing models are commonly referred to as "copyleft" licenses.[109] Some developers fear that using discrete portions of OSS with copyleft licensing requirements in larger development projects can infect the larger project, unintentionally turning a proprietary software product into open source software.[110] While the effect of including copyleft software has not been fully litigated, many developers avoid the use of copyleft software to prevent what they view as unnecessary legal uncertainty.[111] In contrast to copyleft licenses, many OSS licenses are more permissive, and allow the user of the OSS to modify the software or include it in a larger program without a requirement that subsequent distributions follow an open source model.[112] The OSS license that is appropriate for a given situation will vary based on the business need for the software. The open software evolution encouraged by copyleft licensing might benefit users with no intention to modify or sell the licensed software, however, software suppliers who don't want to distribute under the open source model might benefit from more permissive licenses.[113]

In addition to copyright, another concern is the impact OSS can have on trademark rights.[114] To maintain trademark rights in the US, the mark owner must exercise control over the products associated with the mark; so-called 'naked licensing' destroys trademark rights.[115] In other words, if a trademark owner allows entities to freely download, edit, and redistribute OSS bearing the trademark, the trademark owner will have failed to exercise control as required by trademark law. Accordingly, the trademark will be lost. [116] Therefore, it is important to consider the benefits and drawbacks of using a valuable mark on OSS that can be reproduced with limited control by the mark holder.

---

[108] *Id.*

[109] DAVID W. TOLLEN, THE TECH CONTRACTS HANDBOOK 249 (American Bar Association Section of I.P. Law ed., 2d ed. 2015).

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] Tiki Dare and Harvey Anderson, *Passport Without A Visa: Open Source Software Licensing and Trademarks*, International Free and Open Source Software Law Review (2009), http://www.ifosslr.org/ifosslr/article/view/11/37.

[115] *What Is a Naked Trademark License?,* NOLO, https://www.nolo.com/legal-encyclopedia/what-naked-trademark-license.html (last visited Nov. 16, 2017).

[116] *Id.*

Patent Defense Approaches

THE NEED FOR PATENT DEFENSE

With the rapid development of Big Data businesses comes an increased exposure to patent assertion and litigation from both practicing and non-practicing entities.[117] Businesses' "concerns with patent enforcement go beyond NPEs and extend to the disadvantages relative to larger incumbents that [businesses] experience as a result of poor patent quality, high costs, and delays associated with the patent system."[118] As in the past, there is therefore a need to develop patent defense options to ensure companies can innovate and develop their Big Data businesses while minimizing the risk of patent assertion and litigation.

APPROACHES TO PATENT DEFENSE

Several groups and services exist to defend their members and subscribers from patent assertion, thereby minimizing the exposure that comes with developing new Big Data businesses. Some of these include:

- Patent Troll Law Clinic Network (PTLCN) – "aims to provide pro bono services to small companies that have received a demand letters from or been sued by a patent troll";
- Trolling Effects – "a [free] database of troll demand letters that recipients have uploaded";
- PatentFreedom – "[a] database of information about non-practicing entities (NPEs) and the litigation that they bring";
- That Patent Tool – "a [free] website where companies can upload demand letters that they've received from trolls, see demand letters that others have submitted, and anonymously discuss issues related to trolls and demand letters";
- Article One Partners – a "[c]rowd-sourced patent research" service;
- Ask Patents – "a free web service where users both pose questions relating to the patent system and answer the questions of others";
- Defensive Patent License – "an off-the-shelf license that focuses on defensive commitments";
- Open Patent Nonassertion (OPN) Pledge – "an agreement by Google (for now) to not assert certain patents against those using them for open-source software";
- License On Transfer (LOT) Agreement – "every LOT User agrees that when it transfers a patent, the transferred patent automatically becomes licensed to the other LOT Users existing at the time of the transfer";

---

[117] *See generally* Colleen V. Chien, *Patent Assertion and Startup Innovation*, Open Tech. Institute (2013), *available at* https://na-production.s3.amazonaws.com/documents/Patent_Assertion_and_Startup_Innovation_updated.62ca39039688474e9a588fc7019b0dde.pdf.

[118] *Id.* at 22.

- Innovator's Patent Agreement (IPA) – "a commitment from Twitter, and other companies, to their employees that patents can only be used for defensive purposes";
- Docket Navigator – a "[s]earchable online docket database";
- Unified Patents Inc. (Unified) – "NPE assertion and litigation reduction through deterrence";
- Gerchen Keller Capital – "defense-side financing solutions for all types of legal claims, including patent claims";
- RPX – "Preemptive open market patent acquisition";
- IP Claims Management (ipCM) – "[l]itigation financing, management and strategic advisory";
- Open Invention Network (OIN) – "[p]rovides a fully paid-up royalty free license to OIN pro-competitive defensive patent pool in exchange for a commitment to forbear litigation around Linux and to cross-license its own patents to other members";
- Allied Security Trust I (AST) – "[d]efensive patent availability monitoring and purchasing."[119]

In addition to the above services, defensive tactics can be used to guard against patent assertion. For example, employing indemnification clauses in Data Usage Agreements, as discussed further below, or challenging an asserted patent's validity with a post-grant review process (such as *Inter Partes* Review).[120]

Different approaches to warding off NPE's each come with their own pros and cons. Companies should carefully weigh these when deciding whether to join a defensive group, engage a service provider, or employ a defensive tactic.

[119] *Id.* at 52-56.
[120] *See, e.g.*, *id.* at 57-63.

Standard Essential Patents

A standard essential patent is an invention that is necessary to use to comply with an industry or technical standard.[121] If all essential patents are not in the public domain or shared in some way, complying with the technical or industry standard will expose entities to infringement liability.

In the field of Big Data, the technology being developed to capture, store, process, and analyze vast quantities of data could benefit from standardization in order to increase interoperability and the ability to share information. Governments, international bodies[122], academics,[123] and market participants have recognized that the rise of the so called "internet of things" ("IoT") presents one area in particular that will benefit from standardization. As the number of IoT devices continues to increase,[124] industry standards will play a key role in allowing IoT technology to interface across different platforms, markets and manufacturers.[125]

Market participants have already formed alliances and consortia to facilitate standard setting in the IoT industry.[126] These private-sector standards developing organizations ("SDOs") can require participants to disclose any patents they own that would be needed to implement the standard,[127] and can require that these standard essential patents ("SEPs") be licensed to users of the standard on fair reasonable and non-discriminatory terms ("FRAND" terms). Courts from several large jurisdictions, including the U.S., European Union, and China, have recently ruled

---

[121] Robert P. Merges, *An Estoppel Doctrine for Patented Standards*, 1 Cal. L. Rev. 1, 7 (Jan. 1, 2009), available at *http*://scholarship.law.berkeley.edu/mwg-internal/de5fs23hu73ds/progress?id=FCIfhnQ9WfirOUSCrQQEuUKCWTzXB-bVi-YF9CFOluo,&dl.

[122] *See e.g.*, Resolution 98 – Enhancing the Standardization of Internet of Things and Smart Cities and Communities for Global Development, International Telecommunication Union (2016), https://www.itu.int/opb/publications.aspx?lang=en&parent=T-RES-T.98-2016.

[123] *See e.g.*, Thomas H. Davenport & Sanjay E. Sarma, *Setting Standards for the Internet of Things*, Harvard Business Review (Nov. 21, 2014), https://hbr.org/2014/11/setting-standards-for-the-internet-of-things.

[124] Cisco estimates the number of IoT devices could reach 50 billion by 2020. *See* Connections Counter: The Internet of Everything in Motion, Cisco SYS. INC. (July 29, 2013), http://newsroom.cisco.com/featurecontent?articleId=1208342.

[125] *See* Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. Ky. L. Rev. 29, 34 (2016).

[126] *See* A Guide To the Range of Alliances and Consortia Targeting Internet of Things Technology Layers and Industry Verticals, Postscapes https://www.postscapes.com/internet-of-things-alliances-roundup/ (last visited Oct. 12, 2017); Carl Weinschenk, The Who's Who of Internet of Things Standards Bodies (Sept. 15, 2015), https://boundless.aerohive.com/experts/The-Whos-Who-of-Internet-of-Things-Standards-Bodies.html.

[127] *See* Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things* (Jan. 2017), *available at* https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

on the methods for calculating reasonable royalty rates on SEPs with FRAND obligations and the available judicial remedies when negotiations are unsuccessful.[128]

Recognizing the economic potential of the IoT industry, governments have undertaken initiatives to further understand and facilitate expansion of the technology. The U.S. Department of Commerce published a white paper in January 2017 titled "Fostering the Advancement of the Internet of Things," which expressed confidence in private-sector SDOs to make the right choices for the IoT industry.[129] The European Commission conversely has taken a more active role in standard creation and has formed a task force "to perform an IoT Standards landscaping and gap analysis"[130] as part of its initiative to achieve a "Digital Single Market"[131] in the European Union.

While groups have worked to advance standardization in the Big Data industry, a single approach for the future has not emerged. A unified approach might not be feasible because of the breadth of technology required to serve the various needs and functions of a Big Data system. Standards developed to work in one application might not necessarily be optimal for another. Additionally, the complexity and multi-layered nature of Big Data systems can require numerous standards. For example, a Big Data system including technology for "(1) end nodes, (2) connectivity, (3) data centers, (4) analytics/applications, and (5) security" might require five separate standards.[132]

The nascent nature of the Big Data industry can offer opportunities to participate in the standard setting process. Involvement can offer numerous benefits, including strategic and technical influence, early access, training opportunities, joint marketing, and others.[133] However, standard setting is a time consuming and costly endeavor that requires input from many stakeholders to be successful. For example, some estimate that it took 3.5 million

---

[128] *See* Anne Layne-Farrar & Koren W. Wong-Ervin, *Methodologies for Calculating FRAND Damages: An Economic and Comparative Analysis of the Case Law from China, the European Union, India, and the United States*, forthcoming Jindal Global Law School Review (Fall 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985073; Christa Brown-Sanford & Bethany R. Ford, *Post-Huawei FRAND Licensing of Standards-Essential Patents*, Baker Botts (June 2016).

[129] *See* Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things* (Jan. 2017), *available at*https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-thing (Stating that The Department will "defer[] to private sector SDOs to adopt approaches that meet the needs of the participating members and the industries where those standards will be used while appropriately balancing the various interests involved while fairly compensating patent owners for use of their technology.").

[130] *Commission Staff Working Document*, EUR-Lex, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110 (last visited Oct. 31, 2017).

[131] *The Commission to the European Parliament*, EUR-Lex, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15265 (last visited Oct. 31, 2017).

[132] Kenie Ho, *Internet of Things: Another Industry Patent War?* Finnegan (Dec. 2015) https://www.finnegan.com/en/insights/internet-of-things-another-industry-patent-war.html.

[133] Andrew Updegrove, *The Essential Guide to Standards*, Consortium Info.org https://www.consortiuminfo.org/essentialguide/participating1.php (last visited Oct. 31, 2017).

human-hours to develop 3G telecom standards and that industry will need to expend up to $4 trillion to make the European Digital Single Market a reality.[134]

[134] Dugie Standeford, *Special Report: Will the Internet of Things Need New Patenting/Licensing Strategies?*, Lexology (Apr. 3, 2017), https://www.lexology.com/library/detail.aspx?g=2c652d3d-c549-444a-ac36-e3c2ea380a70.

IP Policies

MARKET DEVELOPMENTS IN BIG DATA IP POLICIES

As intellectual property infringement lawsuits arising out of cloud-based applications become more frequent,[135] cloud platform customers have begun to express greater concern that third-parties will sue them alleging infringement related to the customer's use of cloud platforms. [136] Companies like Microsoft, Amazon, Google, GE, and Siemens that offer cloud-based computing solutions have responded to customer concerns largely by trying to provide greater security against third-party intellectual property claims through user agreement amendments. As these developments highlight, it is important to address the risk of IP infringement in data usage agreements.

On February 8, 2017, Microsoft launched its Microsoft Azure IP Advantage Program to protect customers of its Azure cloud services product against third party intellectual property infringement claims.[137] The program protects customers in three ways. First, Microsoft promises to indemnify all users of its Azure platform against claims arising out of their use of the platform.[138] Second, Microsoft's "patent pick" program allows eligible Azure customers who have been sued for patent infringement to select one of 10,000 Microsoft patents to use defensively in that lawsuit.[139] Third, Microsoft grants Azure customers a springing license to any patents that Microsoft may transfer to a non-practicing entity (NPE).[140]

Following Microsoft's Azure launch, Amazon Web Services (AWS) removed a clause from its user agreement that barred users from suing AWS for patent infringement.[141] At the same time, AWS added a clause to its user agreement stating that AWS would defend its customers against third party claims of infringement and indemnify its customers for adverse judgments or settlements.[142]

---

[135] *US Patent Litigation Trends in Cloud Computing,* IP Lytics (Sep. 4, 2017), http://www.iplytics.com/wp-content/uploads/2017/09/IPlytics_Patent-Litigation-Trends-in-Cloud-Computing_2017.pdf.

[136] *Azure IP Advantage,* Microsoft, https://azure.microsoft.com/en-us/overview/azure-ip-advantage/ (last visited Oct. 31, 2017).

[137] Brad Smith, *Protecting innovation in the cloud,* Microsoft (Fed. 8, 2017), https://blogs.microsoft.com/blog/2017/02/08/protecting-innovation-cloud/#sm.0000h85y3pah6fb2z3i16q59eyric.

[138] *See* Azure IP Advantage, *supra* note 136.

[139] *Azure IP Advantage program,* Microsoft, https://www.microsoft.com/en-us/trustcenter/compliance/azureipadvantage (last visited Oct. 31, 2017).

[140] *See* Azure IP Advantage, *supra* note 136.

[141] Tom Krazit, *Amazon Web Services adds IP protection while dropping controversial patent clause from user* agreement, Geek Wire (Jul. 14, 2017) https://www.geekwire.com/2017/amazon-web-services-added-ip-protection-dropping-controversial-patent-clause-user-agreement/.

[142] *AWS Customer* Agreement, Amazon, https://aws.amazon.com/agreement/ (last visited Oct. 31, 2017).

Google's Cloud Platform and GE's Predix license agreements also contain mutual defense and indemnification provisions related to third-party claims of infringement arising out of the use of their respective services.[143] Siemens' MindSphere platform, a cloud-based operating system marketed across many different industries, appears to offer a more tailored service, and potentially different intellectual property policy terms, for each of Siemens' cloud platform clients.[144]

Cloud service providers that pledge to defend their customers against claims of intellectual property infringement put potential plaintiffs on notice that their cloud customers will have support if they are forced to litigate. Accordingly, as major technology companies fight for market share in the cloud computing industry, it is not surprising to see several major cloud platform providers offering similar customer protections through their user agreements and license terms.

Microsoft's three-part promise and other companies' similar mutual defense and indemnity provisions may provide current and prospective cloud customers with a decreased sense of vulnerability to infringement lawsuits. However, schemes like Microsoft's "patent pick" program would likely provide no deterrence against infringement claims brought by non-practicing entities because NPEs have no business operations or products against which defendants could make counterclaims of infringement.

If the frequency of infringement lawsuits against cloud-based applications continues to increase, providers whose policies do not include defense and indemnity provisions could find their customers more vulnerable to suit than customers of other cloud platforms. In that case, policies like indemnification and mutual defense agreements would likely become more common among cloud platform providers. Moreover, while some companies like Amazon, Google, and Microsoft have publicized their intellectual property policies,[145] other companies who have applied similar policies in private may opt for more public strategies to provide greater deterrence against third party intellectual property lawsuits.

---

[143] *Google Cloud Platform Terms of Service,* Google, https://cloud.google.com/terms/ (last modified Oct. 19, 2017) [hereinafter "Google Cloud Platform TOS"]; *Predix Customer Agreement-US,* PREDIX, https://www.predix.io/legal (last modified Aug. 12, 2016).

[144] *MindSphere – open IoT operating system – Software – Siemens Global Website,* Siemens, https://www.siemens.com/global/en/home/products/software/mindsphere.html (last visited Oct. 31, 2017).

[145] *See* Azure IP Advantage, *supra* note 136; AWS Customer Agreement, *supra* note 142; Google Cloud Platform TOS, *supra* note 143.