School of Law
UNIVERSITY OF GEORGIA
Prepare. Connect. Lead.

Journal of Intellectual Property Law

Volume 30 | Issue 2 Article 2

May 2023

Rethinking "Reasonableness": Implementation of a National Board to Clarify the Trade Secret Standard now that the Work-From-Home Culture has Changed the Rules

Hannah E. Brown
hannahebrown90@gmail.com

Rethinking "Reasonableness": Implementation of a National Board to Clarify the Trade Secret Standard now that the Work-From-Home Culture has Changed the Rules

Cover Page Footnote

Senior Associate, Gordon Rees Scully Mansukhani; I thank Trevor Goehring and Dennis Brown for their helpful input and suggestions on earlier drafts.

RETHINKING "REASONABLENESS": IMPLEMENTATION OF A NATIONAL BOARD TO CLARIFY THE TRADE SECRET STANDARD NOW THAT THE WORK-FROM-HOME CULTURE HAS CHANGED THE RULES

Hannah E. Brown[*]

[*] Senior Associate, Gordon Rees Scully Mansukhani; I thank Trevor Goehring and Dennis Brown for their helpful input and suggestions on earlier drafts.

TABLE OF CONTENTS

I. INTRODUCTION

For many of us, it was a memorable week in 2020: one day, we were working in an office with dual computer monitors and an ergonomic chair; the next day, our office had closed, and we were working from our kitchen table on an outdated laptop with our noisy partner working at the same table and our kids attending school remotely in the next room.[1]

The COVID-19 pandemic affected everyone differently, but for many of us, it changed how we worked.[2] Many people were furloughed or lost their jobs due to business shutdowns, and others were forced to change their work situation completely. As of April 2020 — peak pandemic — sixty-two percent of employed Americans worked at home, compared to about twenty-five percent who did so before the pandemic.[3] For those whose jobs remained the same during the pandemic but who were no longer allowed in the office, they were forced to adapt. Some may have been forced to take client calls from a shared workspace or log into the office system using a computer shared by the household.

More employees working from home necessarily means more computers and systems accessing company data, more remote transmissions of information,

---

[1] The date of the work-from-home shift varies per state, but, for example, on March 19, 2020, California Governor Gavin Newsom issued a "stay-at-home order" ordering "all individuals living in the State of California to stay home or at their place of residence except as needed to maintain continuity of operations of the federal critical infrastructure sectors" as detailed in the order. *Exec. Order No. 33-20*, Executive Department State of California (Mar. 19, 2020), https://www.gov.ca.gov/wp-content/uploads/2020/03/3.19.20-attested-EO-N-33-20-COVID-19-HEALTH-ORDER.pdf.

[2] COVID-19 is an abbreviation for coronavirus disease 2019, a disease caused by a virus named SARS-CoV-2. It was discovered in December 2019 in Wuhan, China and quickly spread around the world. *Basics of COVID-19*, CENTERS FOR DISEASE CONTROL AND PREVENTION, https://www.cdc.gov/coronavirus/2019-ncov/your-health/about-covid-19/basics-covid-19.html#:~:text=with%20updated%20guidance.,About%20COVID%2D19,%2C%20a%20flu%2C%20or%20pneumonia (last updated Nov. 4, 2021).

[3] James Urton, *US approaching peak of 'active' COVID-19 Cases, strain on medical resources, new modeling shows*, UW NEWS (Apr. 10, 2020), https://www.washington.edu/news/2020/04/10/covid-19-peak-active-cases/; Brodie Boland et al., *Reimagining the office and work life after COVID-19*, MCKINSEY & CO. (June 8, 2020), https://www.mckinsey.com/business-functions/people-and-organizational-performance/our-insights/reimagining-the-office-and-work-life-after-covid-19.

less secure workspaces, and a large increase in video and phone conversations. In 2019, Zoom had an average of 10 million daily meeting participants, but by 2020, it had 350 million; "to Zoom" had become a verb.[4] An issue that may not have immediately occurred to employers was: "now that almost all my employees are discussing company business from remote locations and sharing confidential documents via email . . . how secure are they being and how safe is our proprietary information?"

Specifically, many companies have trade secrets, a type of intellectual property that is valuable because it is not generally known.[5] Under the federal Defend Trade Secrets Act ("DTSA"), almost any type of information can qualify as a trade secret *but only if* "the owner thereof has taken *reasonable* measures to keep such information secret[.]"[6] This requirement — using the law's most vague unit of measurement[7] — is not defined in the statute, and Congress has not provided guidance on how to interpret this term. What is "reasonable" varies and may differ based on the court, the company size, and the particular facts of each situation.[8] There is abundant pre-pandemic case law addressing the issue with courts around the country analyzing a variety of different fact patterns.[9] However, the widespread increase in working from home poses the question: with more employees working from home — maybe on shared computers or in a less secure space accessible to the public or a family member — will the definition of "reasonable measures" change? Should it?

Part II of this Article provides background information on trade secrets and how courts have addressed what constitutes reasonable measures to protect such

---

[4] Rani Molla, *The pandemic was great for Zoom. What happens when there's a vaccine?*, VOX (Dec. 4, 2020, 11:50 AM), https://www.vox.com/recode/21726260/zoom-microsoft-teams-video-conferencing-post-pandemic-coronavirus. The remote video platform was started in 2012 but took off during the pandemic. Akriti Rana, *7 cool things you might not know about Zoom*, TECHPP, https://techpp.com/2020/05/23/zoom-facts/ (last updated May 23, 2020).

[5] 18 U.S.C. § 1839(3)(B).

[6] *Id.* § 1839(3)(A) (emphasis added).

[7] *See* Omnicare, Inc. v. Laborers Dist. Council Constr. Indus. Pension Fund, 575 U.S. 175, 194 (2015) ("Numerous legal rules hinge on what a reasonable person would think or expect."); *see generally* Kevin P. Tobia, *How People Judge What is Reasonable*, 70 ALA. L. REV. 293 (2018) (analyzing various theories of reasonableness).

[8] Some courts or statutes broadly provide that the efforts to maintain the secrecy of the information must be "reasonable *under the circumstances*." Indus. Packaging Supplies, Inc. v. Davidson, No. CV 6:18-0651-TMC, 2018 WL 10456201, at *4 (D.S.C. June 22, 2018) (emphasis added); *see also* Va. Code Ann. § 59.1-336 (West 2009) (providing a trade secret must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy"). This indicates "reasonable" could mean different things for different companies and that courts should evaluate the standard differently based on the company itself.

[9] *See supra* Section II.C.

secrets. Part III discusses the recent shift in the American work-life landscape, namely the upsurge in teleworking and other changes in today's digital era. Part IV describes the issue this poses for two reasons: because companies have not adapted their security and technology to keep up with the rise in remote work and protect their proprietary intangible information and because courts have not changed their analysis to require certain seemingly "reasonable" actions. Part V suggests a solution, a national board that sets a standard for companies to follow so that they may engage in sufficiently "reasonable" protection efforts. If followed, the standard provides a presumption of "reasonable measures" under the DTSA.

II. BACKGROUND ON TRADE SECRETS AND "REASONABLE" MEASURES TO PROTECT THEM

A. WHAT IS A TRADE SECRET?

The most common reason courts evaluate trade secrets is under a claim of trade secret misappropriation. Misappropriation was governed only by state law until 2016 when Congress enacted the DTSA, creating a federal private right of action for trade secret misappropriation.[10] Many states have enacted their own trade secret laws, but the DTSA provides a national uniform cause of action for misappropriation.[11]

Under the DTSA, one form of misappropriation is via "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[.]"[12] The term "improper means" includes "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means[.]"[13] For a plaintiff to prove misappropriation, it must initially prove there is

[10] *Explaining the Defend Trade Secrets Act*, A.B.A. (Sept. 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/09/03_cohen/.
[11] *Id.*
[12] 18 U.S.C. § 1839(5)(A). Certain state laws have expanded this definition. For example, "a plaintiff can state a claim for misappropriation of trade secrets under Pennsylvania law even where the trade secret was acquired by mistake rather than misconduct." Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. CIV.A. 07-1029, 2007 WL 4394447, at *8 (E.D. Pa. Dec. 13, 2007).
[13] 18 U.S.C. § 1839(6)(A).

something to misappropriate, i.e., that it has a trade secret to begin with.[14] Establishing and identifying one's trade secrets is the first step in being able to protect them.[15]

The DTSA's definition of a trade secret does not specify the format or subject matter of the secret, however, case law shows that trade secrets are most often intangible.[16] The DTSA lists examples of trade secrets as "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 "[17] Courts have expanded these examples, finding that a trade secret can be, inter alia, marketing plans and analysis;[18] a compilation of customer, operator, and vendor information;[19] customer lists[20] (alone or with pricing and sales information),[21] prototypes,[22] software, source code, user manuals,[23] and recipes.[24] The most famous trade secrets include the original recipe for Coca-Cola, the ingredients for Kentucky Fried Chicken's original spice recipe, and the Google search algorithm.[25]

---

[14] *See* Cherokee Chem. Co. v. Frazier, No. CV 20-1757-MWF (ASx), 2020 WL 8410432, at *3 (C.D. Cal. Dec. 14, 2020) ("To state a claim for trade secret misappropriation under the DTSA, a plaintiff must allege: "(1) the existence and ownership of a trade secret, and (2) misappropriation of the trade secret." (quoting Sun Distrib. Co. v. Corbett, No. 18-CV-2231-BAS-BGS, 2018 WL 4951966, at *3 (S.D. Cal. Oct, 12, 2018))).

[15] PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co., No. 2:15-CV-00965, 2020 WL 1526940, at *14 (W.D. Pa. Mar. 31, 2020).

[16] Coast Hematology-Oncology Assocs. Med. Grp., Inc. v. Long Beach Mem'l Med. Ctr., 272 Cal. Rptr. 3d 715, 722 (Cal. Ct. App. 2020) ("[I]ntellectual property is intangible.").

[17] 18 U.S.C. § 1839(3).

[18] Yeiser Rsch. & Dev., LLC v. Teknor Apex Co., No. 17-CV-1290-BAS-RBB, 2018 WL 3993370, at *5 (S.D. Cal. Aug. 21, 2018) (citations omitted).

[19] Pyro Spectaculars N., Inc. v. Souza, 861 F. Supp. 2d 1079, 1088–89 (E.D. Cal. 2012).

[20] Marina Dist. Dev. Co., LLC v. AC Ocean Walk, LLC, No. 22-CV-01592-GMN-BNW, 2020 WL 5502160, at *3 (D. Nev. Sept. 10, 2020) (citations omitted).

[21] Freedom Med. Inc. v. Whitman, 343 F. Supp. 3d 509, 515 (E.D. Pa. 2018); *see also* COLO. REV. STAT. ANN. § 7–74–102(4) (defining trade secret to include the "listing of names, addresses, or telephone numbers, or other information relating to any business or profession which is secret and of value").

[22] Heska Corp. v. Qorvo US, Inc., No. 1:19CV1108, 2020 WL 5821078, at *5 (M.D.N.C. Sept. 30, 2020) (citations omitted).

[23] Comput. Scis. Corp. v. Tata Consultancy Servs. Ltd., No. 3:19-CV-970-X(BH), 2020 WL 2487057, at *4 (N.D. Tex. Feb. 7, 2020); Scott Env't Servs., Inc. v. Newfield Expl. Co., No. 2:19-CV-0026-JRG-RSP, 2019 WL 6220968, at *2 (E.D Tex. Oct. 23, 2019).

[24] Bambu Franchising, LLC v. Nguyen, 537 F. Supp. 3d 1066, 1073 (N.D. Cal. 2021).

[25] *Trade Secrets: 10 of the Most Famous Examples*, VETHAN L. FIRM (Nov. 8, 2016), https://info.vethanlaw.com/blog/trade-secrets-10-of-the-most-famous-examples. A lesser-

A trade secret is, of course, "secret," meaning generally it is not publicly available and a third party cannot simply look it up or figure it out. A trade secret also cannot be something that "any user or passer-by sees at a glance[,]" such as an item's appearance or a screen display.[26] However, courts are split on whether a trade secret can consist of publicly available information. Some courts say yes.[27] In that analysis, even if isolated pieces of the trade secret information can be found publicly, the compiled list or the "minute details" of that information can nevertheless constitute a trade secret.[28] Other courts disagree, finding that if the list of information is obtainable by compiling public information, the information cannot be a trade secret.[29]

---

known example of a trade secret owned by Coca-Cola is the formulation for bisphenol-A (BPA)-free coatings for the insides of cans. Rebecca Trager, *Former Coca-Cola chemist imprisoned for trade secret theft*, CHEMISTRY WORLD (May 12, 2022), https://www.chemistryworld.com/news/former-coca-cola-chemist-imprisoned-for-trade-secret-theft/4015661.article. In fact, a former Coca-Cola chemist received a 14-year prison sentence for conspiring to steal that trade secret. *Id.*

[26] InteliClear, LLC v. ETC Glob. Holdings, Inc., 978 F.3d 653, 660 (9th Cir. 2020) (citing IDX Sys. Corp. v. Epic Sys. Corp., 285 F.3d 581, 584 (7th Cir. 2002)).

[27] Power Home Solar, LLC v. Sigora Solar, LLC, No. 20 CVS 7165, 2021 WL 2530984, at *14 (N.C. Super. Ct. June 18, 2021) (citations omitted) ("[A] compilation of publicly available information may be a protectible trade secret under . . . the DTSA."); IHS Glob. Ltd. v. Trade Data Monitor, LLC, No. 2:18-CV-01025-DCN, 2021 WL 2134909, at *8 (D.S.C. May 21, 2021) (citations omitted) (finding the DTSA "offers trade secret protection to compilations of publicly available information . . .").

[28] United States v. Liew, 856 F.3d 585, 603 (9th Cir. 2017) (finding that while "the basic concept of chlorination, oxidation, and finishing is the same" at DuPont's facility as at other facilities and thus may be generally known, "it was the minute details and data involved in DuPont's technology that merited trade secret status, not the 'basic concept' of the chloride process"); Woven Elecs. Corp. v. Advance Grp., Inc., 1991 WL 54118, at *3 (4th Cir. Apr. 15, 1991) (finding "evidence that some of the technology may have been public knowledge . . . does not defeat [plaintiff's] claims" that it constituted a trade secret).

[29] Free Country Ltd. v. Drennen, 235 F. Supp. 3d 559, 566 (S.D.N.Y. 2016) (finding plaintiff's customer list was not a trade secret because the contact information for the companies was "readily ascertainable" via phone calls, the internet, and directories of buyers in the apparel industry); Kadant, Inc. v. Seeley Mach., Inc., 244 F. Supp. 2d 19, 36 (N.D.N.Y. 2003) (citations omitted) (finding list of specific names of individuals key to the purchasing chain of command was not a trade secret where customer companies' general contact information was readily available and "follow-up questions to the company in general would reveal the specific names, e-mail addresses, or phone numbers of individuals involved in the purchasing process . . ."); RF Techs. Corp. v. Applied Microwave Techs., Inc., 369 F. Supp. 2d 17, 22 (D. Me. 2005) (finding information does not qualify as trade secrets when

In sum, the definition of a trade secret under the DTSA consists of three elements: (1) information, (2) that is valuable because it is unknown to others, and (3) that the owner has attempted via reasonable measures to keep secret.[30] State law definitions may vary slightly, but the requirement that the trade secret owner makes a "reasonable" effort to maintain the information's secrecy is consistently applied.[31]

B. PROTECTING TRADE SECRETS

With any property right comes the right to exclude others from using it.[32] Applying this right to tangible property is simple; one knows the boundaries of their land or chattels and can prevent others from entering or using that property. If a person owns a bicycle, they know that they can prevent others from using that bicycle; it is not confusing which, or how many, bicycles they own or can claim the right to use. In contrast to tangible property, trade secrets, for the most part, are nonphysical and intangible,[33] and therefore ownership of them is not as easily defined. "One cannot use a yardstick to measure the boundaries of inventions and proprietary information."[34]

Some intangible intellectual property is easier to measure. For example, a copyright protects an original work of authorship fixed in a tangible medium of expression,[35] and the "work of authorship" defines what the owner can protect.[36] If an artist creates a painting, that painting is the work of authorship and is a

"[p]laintiffs have provided no evidence . . . that trained microwave engineers would not be aware of these sources or be able to find this information").

[30] InteliClear, 978 F.3d at 657 (citing 18 U.S.C. § 1839(3)). Various state laws further require that the trade secret give the owner a competitive advantage over those who do not know the information. Rothschild v. Ford Motor Co., 2 F. Supp. 2d 941, 950 (E.D. Mich. 1998) (Michigan law); 3M v. Pribyl, 259 F.3d 587, 595–96 (7th Cir. 2001) (Wisconsin law).

[31] *See, e.g.*, MD. CODE ANN., COM. LAW § 11-1201(e) (West 2010); CAL. CIV. CODE § 3426.1(d) (West 2012); FLA. STAT. ANN. § 688.002(4) (West 1998); OHIO REV. CODE ANN. § 1333.61(B) (West 1994); GA. CODE ANN. § 10-1-761(4) (West 2022); CONN. GEN. STAT. ANN. § 35–51(d) (West 1995); N.C. GEN. STAT. ANN. § 66-152(3) (West 1981).

[32] Ralphs Grocery Co. v. Victory Consultants, Inc., 17 Cal. App.5th 245, 258 (2017) (finding the right to exclude is a fundamental aspect of property ownership).

[33] Coast Hematology-Oncology Assocs. Med. Grp., Inc. v. Long Beach Mem'l Med. Ctr., 272 Cal. Rptr. 3d 715, 722 (Cal. Ct. App. 2020) ("[I]ntellectual property is intangible.").

[34] *Id.*

[35] 17 U.S.C. § 102(a).

[36] Coast Hematology-Oncology, 272 Cal. Rptr. 3d at 722 (citing 17 U.S.C. § 102(a)).

physical manifestation of what the copyright protects.[37] Moreover, the owner of a common law trademark can protect its rights in the geographic area where it uses the mark and in connection with specific goods or services.[38] Similarly, the owner of a registered trademark can protect the goods or services listed on the registration.[39]

Trade secrets are different and do not need to be tangible, written down, or used for them to be protected or to exist. "No physical ruler can measure a [trade] secret in inches or yards."[40] Therefore, "the extent of the property right [of a trade secret] is defined by the extent to which the owner of the secret protects his interest from disclosure to others."[41] A trade secret is measured by its value, and a trade secret is only valuable if it is unknown and unknowable to others.[42]

For this reason, trade secrets are generally not protectable by other forms of intellectual property.[43] For example, the Coca-Cola recipe is a trade secret, and the company intentionally chose not to patent the recipe.[44] This is because patents do not last forever; for the duration of a patent, which is fifteen or twenty years, the inventor has the sole right to sell, make, distribute, and license that

---

[37] *Id.* ("When Willa Cather published *My Ántonia*, for instance, her novel fixed her work of authorship and marked out her copyright for the world to inspect and admire."). However, a copyright can be infringed if the work of authorship is copied on another medium. *See generally* Home Art Inc. v. Glensder Textile Corp., 81 F. Supp. 551 (S.D.N.Y. 1948) (discussing an oil painting reproduced in scarf); Leigh v. Gerber, 86 F. Supp. 320 (S.D.N.Y. 1949) (discussing a painting reproduced by publication without consent in a magazine).

[38] Benjamin D. Schwartz, *Common Law v. Federally Registered Trademark Rights*, THE NAT'L L. REV. (May 6, 2022), https://www.natlawreview.com/article/common-law-v-federally-registered-trademark-rights.

[39] *Trademark scope of protection*, USPTO, https://www.uspto.gov/trademarks/basics/scope-protection (last visited Nov. 13, 2022).

[40] 1 MELVIN F. JAGER, TRADE SECRETS LAW § 4:3 (Oct. 2022).

[41] Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) (citations omitted).

[42] Miranda v. Thiry, No. 2:20-CV-05527-ODW-(KESx), 2021 WL 5760299, at *4 (C.D. Cal. Dec. 2, 2021) (citations omitted) ("A trade secret is valuable *because* it is unknown and unknowable to others who might find it valuable.").

[43] Subscriber Holdings, LLC v. Brightstar Corp., No. 1:19-CV-1991-TWT, 2021 WL 3926258, at *5 (N.D. Ga. July 28, 2021) ("Disclosure of a trade secret in a patent destroys its value."), *vacated*, No. 21-12985, 2022 WL 18034431 (11th Cir. Dec. 30, 2022).

[44] In 1893, Coca-Cola patented its original formula, but after the formula changed, Coca-Cola chose not to patent the new formula. Maria Cruz, *Coca-Cola Never Actually Patented Their Secret Formula – Here's Why*, OOLA (Aug. 13, 2018), https://www.oola.com/life-in-flavor/2455512/coca-cola-never-actually-patented-their-secret-formula-heres-why/.

product.[45] However, after the patent expires, it becomes a part of the public domain and can be usable by anyone.[46] Accordingly, if Coca-Cola had patented its recipe, the recipe would be disclosed once the patent expired, and it could not be a trade secret. Instead, the new Coca-Cola formula is maintained only as a trade secret. If reasonable measures are used to keep the formula a secret, it can be protected indefinitely.[47]

Trade secrets can be copyrighted, but only if a specific procedure is followed.[48] For example, many computer programs and their source code are protected by both copyright and trade secret law.[49] The Copyright Office has special procedures for registering computer programs that contain trade secrets, and the applicant can redact the proprietary code within the copyright application to ensure that application does not publicly disclose the trade secret.[50]

Further, under certain circumstances, a trade secret can be lost even if its disclosure is via third-party misappropriation.[51] For example, in one case, Religious Technology Center v. Netcom On-Line Communication Services, Inc., the plaintiff was a religious corporation that considered written work by its founder to be trade secrets.[52] Defendant Erlich was a former church minister, and he posted those works on an online forum, and the church sued him for misappropriation.[53] Erlich claimed that someone else had previously anonymously posted the works on the Internet and, therefore, could not qualify

---

[45] 35 U.S.C. § 154(a)(2) (utility patents); 35 U.S.C. § 173 (design patents).
[46] *Why Do Patents Expire: Everything You Need to Know*, UPCOUNSEL, https://www.upcounsel.com/why-do-patents-expire (last visited September 1, 2022).
[47] *Understanding Intellectual Property Law Through Coca Cola*, ZVULONY & CO (Dec. 1, 2010), https://zvulony.ca/2010/articles/intellectual-property-law/understanding-intellectual-property-law/. Apparently, "[n]o single contractor has the full recipe; each is tasked to prepare only parts of the classic blend. The company has kept the secret for over a century by purportedly storing it in a vault in downtown Atlanta, and restricting access to only a handful of executives." Orly Lobel, *Filing for a Patent Verses Keeping Your Invention a Trade Secret*, HARVARD BUSINESS REVIEW (Nov. 21, 2013), https://hbr.org/2013/11/filing-for-a-patent-versus-keeping-your-invention-a-trade-secret.
[48] Woodall v. Walt Disney Co., No. CV 20-3772-CBM-(EX), 2021 WL 4442410, at *2 (C.D. Cal. Aug. 5, 2021) (citations omitted) (finding "information regarding Plaintiff's . . . works which were . . . deposited with the Copyright Office were not trade secrets").
[49] *Copyright Registration of Computer Programs*, U.S. COPYRIGHT OFF. 3, https://www.copyright.gov/circs/circ61.pdf?loclr=blogcop (last updated Mar. 2021).
[50] *Id.* at 4.
[51] Hong Kong uCloudlink Network Tech. Ltd. v. Simo Holdings Inc., No. 18-CV-05031-EMC, 2019 WL 1767329, at *1 (N.D. Cal. Apr. 22, 2019); Forcier v. Microsoft Corp., 123 F. Supp. 2d 520, 528 (N.D. Cal. 2000).
[52] Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1239 (N.D. Cal. 1995).
53 *Id.*

as trade secrets.[54] The court agreed, finding that because another individual had put the works into the public domain, the plaintiff was prevented from further enforcing its trade secret rights in those materials.[55] There is a caveat available; a non-owner's unauthorized public disclosure of a trade secret cannot shield a second misappropriator against liability if the second knew the trade secret was misappropriated[56] or if the two misappropriators were in privity with each other.[57] In Religious Technology Center, however, because there was no evidence that Erlich was in privity with any of the alleged original misappropriators, he could raise that prior disclosure as a defense.[58] Because of this, the plaintiff could not succeed on its misappropriation claim.[59]

A result like this may seem unfair to a trade secret owner who may have done nothing wrong, and it means that theft of information can permanently remove that information from the category of "trade secret." But, the result is logical. Because trade secrets only exist if they have value, the law requires the owner to put in at least some effort (i.e., a "reasonable" amount) to protect the trade secrets: "Trade secret law does not help those who fail to help themselves . "[60] And, because a trade secret loses value if not kept a secret, once the cat is out of the bag, it cannot be put back in. To put it in non-idiom terms: "once that trade secret has been released into the public domain[,] there is no retrieving it."[61] Knowing that even an unintentional disclosure can deprive the owner of valuable property further incentives them to exert even more than reasonable measures to protect their information.

C. WHAT ARE "REASONABLE MEASURES"?

Pre-pandemic, countless federal courts analyzed and did their best to determine what a company must do to "reasonably" protect its confidential

54 *Id.* at 1239-40.
55 *Id.* at 1256.
56 Houser v. Feldman, 569 F. Supp. 3d 216, 227 (E.D. Pa. 2021) (citations omitted).
57 Underwater Storage, Inc. v. U.S. Rubber Co., 371 F.2d 950, 955 (D.C. Cir. 1966). ("Once the secret is out, the rest of the world may well have a right to copy it at will; but this should not protect the misappropriator or his privies.").
58 Religious Tech. Ctr., 923 F. Supp. at 1256-57.
59 *Id.* at 1257.
60 Courtney M. Cox, *Legitimizing Lies*, 90 GEO. WASH. L. REV. 297, 320 (2022).
61 Religious Tech. Ctr., 923 F. Supp. at 1256 (citations omitted).

information under the DTSA. Overall, a business "is not required to turn itself into an 'impenetrable fortress' to protect its trade secrets[,]"[62] however, its efforts must be more than minimal.[63] The company must treat the information differently than it treats "any other corporate information."[64]

Courts tend to agree that the DTSA term "reasonable efforts" is not clearly or universally defined.[65] Nor is this an issue that courts will decide early in a case because "[w]hether a party's efforts are 'reasonable' is ordinarily an issue for the trier of fact."[66] This undefined standard is interpreted differently by different courts, but with the following factors making an appearance in many cases.

1. Physical Marking of the Documents

The first often-analyzed issue in a reasonableness analysis is the physical marking of the documents to indicate their confidential status. One court found that "an employer's failure to mark documents as confidential or trade secret 'precludes in many cases trade secret protection for those materials.'"[67] Many courts have agreed, reasoning that because documents are now often and most likely shared via a digital format, affixing a confidential designation to the documents is needed to ensure the receiver clearly understands the confidentiality.[68] On the other hand, other courts have found that failure to mark documents as confidential is only a factor to consider in the reasonableness

[62] Pyro Spectaculars N., Inc. v. Souza, 861 F. Supp. 2d 1079, 1091 (E.D. Cal. 2012) (citations omitted).
[63] *See* USM Corp. v. Marson Fastener Corp., 393 N.E.2d. 895, 899 (Mass. 1979) ("One who possesses a trade secret and wishes to protect it must act to preserve its secrecy.").
[64] Opus Fund Servs. (USA) LLC v. Theorem Fund Servs., LLC, No. 17 C 923, 2018 WL 1156246, at *3 (N.D. Ill. Mar. 5, 2018).
[65] United States v. Shanshan Du, 570 F. App'x 490, 500 (6th Cir. 2014) ("There is not a single definition for what constitutes 'reasonable measures' ....."); ClearOne Commc'ns, Inc. v. Bowers, 643 F.3d 735, 768 (10th Cir. 2011) ("There is no precise definition of what 'reasonable measures' are; what is reasonable depends on the situation.").
[66] Workplace Techs. Rsch., Inc. v. Project Mgmt. Inst., No.: 18CV1927 JM (MSB), 2021 WL 4895977, at *22 (S.D. Cal. Oct. 20, 2021) (citations omitted); *see also In Re* Providian Credit Card Cases, 116 Cal. Rptr. 2d 833, 844 (Cal. Ct. App. 2002) ("[W]hether a party claiming a trade secret undertook reasonable efforts to maintain secrecy is a question of fact."); InfoSpan, Inc. v. Emirates NBD Bank PJSC, No. SACV 11-1062 JVS (ANx), 2015 WL 13357646, at *3 (C.D. Cal. May 6, 2015) (citations omitted) ("The reasonable efforts analysis is a 'fact intensive' one.").
[67] Mattel, Inc. v. MGA Ent., Inc., 782 F. Supp. 2d 911, 959 (C.D. Cal. 2011)(quoting Gemisys Corp. v. Phoenix Am., Inc., 186 F.R.D. 551, 559 (N.D. Cal. 1999)).
[68] Physiotherapy Assocs., Inc. v. ATI Holdings, LLC, 592 F. Supp. 3d 1032, 1042 (N.D. Ala. 2022)).

analysis but is "not dispositive."[69] As is true for many of the factors analyzed herein, these different rulings make it difficult for a company to know what it must do to sufficiently protect its trade secrets.

2. Employee Access to Trade Secrets

Another issue courts often analyze in evaluating reasonableness is how companies share their trade secrets with employees. It is a given that employees will need to access their employers' trade secrets, and companies, therefore, must determine how to manage that access and what to require before allowing it. If the owner discloses the trade secret to anyone, even an employee, who is "under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished."[70]

Overall, a confidential disclosure (as long as that confidentiality is clear in one way or another) to employees does not turn a trade secret into a non-trade secret.[71] In evaluating this, courts often consider whether the employees sign confidentiality agreements before receiving the trade secrets. Some courts find that companies must have an express confidentiality agreement with their

[69] Workplace Techs. Rsch., 2021 WL 4895977, at *23; *see also In re* Providian Credit Card Cases, 116 Cal. Rptr. 2d at 842 ("[A]mong the factors repeatedly noted are restricting access and physical segregation of the information, confidentiality agreements with employees, and marking documents with warnings or reminders of confidentiality.").

[70] Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984).

[71] United States v. Nosal, 844 F.3d 1024, 1043–44 (9th Cir. 2016) (citations omitted) ("It is also well established that 'confidential disclosures to employees, licensees, or others will not destroy the information's status as a trade secret.'").

employees to sufficiently protect the information.[72] Informing the employees of the documents' secrecy, without more, is not enough.[73]

In contrast, other courts have determined that "a confidentiality agreement is not an absolute prerequisite to trade secret protection" if other measures make up for the lack of an agreement.[74] These courts find that limiting access to information to employees on a "need to know basis" and verbally telling the recipients the information is confidential may negate the need for a confidentiality agreement.[75] Regardless, it seems an employer's failure to somehow inform its employee recipients of their obligation to keep certain information a secret or advise them that the company considers the information to be proprietary will almost certainly prevent that information from being deemed a trade secret under the DTSA.[76]

As noted, some companies limit the receipt of trade secrets on a "need to know basis,"[77] but this is not a requirement. For example, in one case, a company considered its training materials to be trade secrets; however, it allowed its affiliates to publish the training materials on their Facebook pages.[78] The

[72] Mintz v. Mktg. Cohorts, LLC, No. 18-CV-4159 (ERK) (SIL), 2019 WL 3337896, at *6 (E.D.N.Y. July 25, 2019) (determining that a misappropriation claim failed in part because plaintiff "did not require defendants to sign a non-disclosure agreement nor any sort of covenant to protect" the alleged trade secret); *see also* Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1550 (11th Cir. 1996) (holding that, absent a written confidentiality agreement, a "unilateral assertion" of "an implied confidential relationship" was insufficient evidence to demonstrate "reasonable efforts"); Yellowfin Yachts, Inc. v. Barker Boatworks, LLC, 898 F.3d 1279, 1299–301 (11th Cir. 2018) (finding that the plaintiff's internal information security measures were not "reasonable efforts" given lack of express confidentiality agreement and minimal evidence of implied confidential relationship).

[73] Charles Ramsey Co. v. Fabtech-NY, No. 1:18-CV-0546 (LEK/CFH), 2020 WL 352614, at *15 (N.D.N.Y. Jan. 21, 2020); *see also* Altman Stage Lighting, Inc. v Smith, No. 20 CV 2575 (NSR), 2022 WL 374590, at *5 (S.D.N.Y. Feb. 8, 2022) ("While Plaintiff alleges employees were instructed not to discuss the Grow Light, without more, the [complaint] has failed to allege or show Plaintiff took reasonable measures to keep the product secret.").

[74] PEO Experts CA, Inc. v. Engstrom, No. 2-17-CV-00318-KJM-CKD, 2017 WL 4181130, at *6 (E.D. Cal. Sept. 21, 2017) (citations omitted).

[75] Graduation Sols. LLC v. Luya Enter., No. CV 19-1382-DMG (JPRx), 2020 WL 9936697, at *11 (C.D. Cal. May 5, 2020) (quoting Hilderman v. Enea TekSci, Inc., 551 F. Supp. 2d 1183, 1201 (S.D. Cal. 2008)).

[76] Payward, Inc. v. Runyon, No. 20-CV-02130-MMC, 2021 WL 242903, at *3 n.5 (N.D. Cal. Jan. 25, 2021); *see also* United States v. Chung, 659 F.3d 815, 825–26 (9th Cir. 2011) ("[R]easonable measures for maintaining secrecy have been held to include advising employees of the existence of a trade secret ").

[77] Graduation Sols., 2020 WL 9936697, at *11.

[78] Tori Belle Cosms. LLC v. McKnight, No. C21-0145RSL, 2022 WL 3927069, at *4 (W.D. Wash. Aug. 31, 2022).

affiliates were independent contractor salespeople selling the company product.[79] In recruiting and training more salespeople, these affiliates shared the training materials via private Facebook groups.[80] The court held there was no issue with sharing the information with outside affiliates, but, because the groups in which the affiliates shared the trade secrets were not limited to those who had agreed to keep the information confidential, the materials were not reasonably kept in confidence and could not be considered trade secrets.[81] Overall, case law does not set a limit on exactly who may access the information, and what is more important is how it is shared, i.e., under the protection of confidentiality.

3. Sharing Trade Secrets With Non-Employees

Companies often provide their trade secrets not only to their employees but also to outside customers, contractors, experts, potential business ventures, and more. While sharing trade secrets with these third parties does not prevent the information from being a trade secret, companies must endeavor to ensure these third parties understand that the information is confidential and cannot be shared with others.[82] Similar to the standard for sharing trade secrets within a company, some courts have held that before sharing the documents with outside third parties, trade secret owners must "require [the receiver] to sign a non-disclosure agreement [or] any sort of covenant to protect" the alleged secrets for the company's efforts to be deemed reasonable.[83] But, other courts have found that a written confidentiality agreement is not required between the trade secret

[79] *Id.* at *1-2.
[80] *Id.* at *4.
[81] *Id.* at *7.
[82] Vendavo, Inc. v. Long, 397 F. Supp. 3d 1115, 1132 (N.D. Ill. 2019).
[83] Mintz v. Mktg. Cohorts, LLC, No. 18-CV-4159 (ERK) (SIL), 2019 WL 3337896, at *6 (E.D.N.Y. July 25, 2019) (citations omitted); *see also* Mason v. AmTrust Fin. Servs., Inc., No. 19CV8364 (DLC), 2020 WL 1330688, at *3 (S.D.N.Y. Mar. 23, 2020) (granting motion to dismiss misappropriation claim where plaintiff did not require any written contract before handing the product in question over to the defendant for its use); Charles Ramsey Co. v. Fabtech-NY LLC, No. 1:18-CV-0546 (LEK/CFH), 2020 WL 352614, at *16 (N.D.N.Y. Jan. 21, 2020) (providing that where complaint contained no allegations of contractual confidentiality agreements).

owner and the receiver as long as there is "an understanding of confidentiality" between them.[84]

In one case, a company's code of conduct required employees to keep the information confidential and to ensure customers signed a confidentiality agreement before sharing proprietary information with those customers.[85] But litigation revealed that a company employee did not, in fact, require customers to sign a confidentiality provision or restrict the customers from sharing the information with others.[86] As a result, the court found the company had not sufficiently protected its information, and this was one reason the information did not qualify as a trade secret.[87]

This court decision seems to set a high bar, as other courts have held that the company's procedures need not be perfect because there is no way to completely prevent information from being shared.[88] The company must simply make a reasonable attempt to do so, and the fact that its efforts fail does not necessarily mean the procedures were unreasonable.[89]

---

[84] DePuy Synthes Prods., Inc. v. Veterinary Orthopedic Implants, Inc., 990 F.3d 1364, 1372 (Fed. Cir. 2021) ("[T]he lack of an express confidentiality agreement is not dispositive.").
[85] Westrock Co. & Victory Packaging, LP v. Dillon, No. 21-CV-05388, 2021 WL 6064038, at *10 (N.D. Ill. Dec. 22, 2021).
[86] *Id.*
[87] *Id.*; *see also* Fire 'Em Up, Inc. v. Technocarb Equip. (2004) Ltd., 799 F. Supp. 2d 846, 851 (N.D. Ill. 2011) (citations omitted) ("While 'an agreement restricting the use of information [by the receiver] may be considered a reasonable step to maintain secrecy of a trade secret, . . .' such an agreement, without more, is not enough.").
[88] Pyro Spectaculars N., Inc. v. Souza, 861 F. Supp. 2d 1079, 1091 (E.D. Cal. 2012) ("While [plaintiff's] security practices are not perfect and these issues can certainly be explored further in discovery and at trial, the court finds for purposes of this [preliminary injunction] motion that [plaintiff] has made reasonable efforts to maintain the secrecy of the information in its [alleged trade secret]."); Comput. Assocs. Int'l v. Quest Software, Inc., 333 F. Supp. 2d 688, 696 (N.D. Ill. 2004) (finding that trade secret owners need only take reasonable — "not perfect[]" — measures to maintain secrecy).
[89] Albert S. Smyth Co. v. Motes, No. CV CCB-17-677, 2018 WL 3635024, at *4 (D. Md. July 31, 2018); *see also* United States v. Liew, 856 F.3d 585, 601 (9th Cir. 2017) ("[T]he government was not required to prove that no disclosures of DuPont's . . . technology occurred. Instead, it needed to establish that DuPont took reasonable measures to guard that technology."). But, this is contrary to the case law noted herein that holds just one misappropriation of a trade secret can mean the trade secret status is destroyed. *See supra* text accompanying notes 52 -55, 58-59, 61 (discussing Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1254 (N.D. Cal. 1995)).

4. Secure Storage of the Information

Another issue courts consider in analyzing what constitutes "reasonable measures" is the physical security and safe storage of trade secret information.[90] Many courts find companies must treat trade secrets differently than they treat other corporate or proprietary information; simply storing the information in a password-protected drive is not enough to qualify as reasonable because that approach is "deployed by nearly all businesses today "[91] Indeed, at least one court found that failing to store information in a password-protected location necessarily means the company was not acting reasonably to protect it.[92] On the other hand, another court found storing documents in a password-protected location is not a required factor in the "reasonableness" analysis as long as the company's actions overall are reasonable.[93] One court even found that all trade secrets need not be in a sure system and held at the motion to dismiss stage that it is reasonable if a company maintains computer login procedures and password protection "for at least some of the information" it deems trade secrets.[94]

5. Employee Access to Information Following Termination

A final consideration in the "reasonableness" analysis concerns the measures taken to protect trade secrets when an employee with access to trade secrets leaves the company. If a departing employee had access or could still access trade secrets, the company must ensure it revokes all access to its system and that the

[90] Charles Ramsey Co., Inc. v. Fabtech-NY LLC, No. 1:18-CV-0546 (LEK/CFH), 2020 WL 352614, at *15 (N.D.N.Y. Jan. 21, 2020) (citing United States v. Shanshan Du, 570 F. App'x 490, 500 (6th Cir. 2014)).

[91] Inv. Sci., LLC v. Oath Holdings Inc., No. 20 CIV. 8159 (GBD), 2021 WL 3541152, at *4 (S.D.N.Y. Aug. 11, 2021); *see also* Physiotherapy Assocs. v. ATI Holdings, 592 F. Supp. 3d 1032, 1041 (N.D. Ala. 2022) ("[T]he use of password-protected servers shows reasonable secrecy *only* when paired with other substantial efforts.").

[92] *See* Boston Laser, Inc. v. Zu, No. 3:07-CV-0791, 2007 WL 2973663, at *10, *12 (N.D.N.Y. Sept. 21, 2007) (finding that plaintiff had not taken reasonable measures to preserve secrecy where, among other things, "the computer network on which such matters are digitally stored is generally not even password protected beyond the log-in process").

[93] Workplace Techs. Rsch., Inc. v. Project Mgmt. Inst., Inc., No.: 18CV1927 JM (MSB), 2021 WL 4895977, at *23 (S.D. Cal. Oct 20, 2021).

[94] TMX Funding, Inc. v. Impero Techs., Inc., No. C 10-00202 JF (PVT), 2010 WL 2509979, at *4 (N.D. Cal. June 17, 2010).

employee did not take any trade secrets with them.[95] There is no bright line defining exactly when these steps must occur following termination, and case law simply (and rather unhelpfully) holds the company must act "reasonably" or "swiftly" to terminate the employee's access.[96] This likely means it must happen within two to three days after the employee's departure.[97]

6. Summary of Main Factors

Given all available avenues of protection, the million dollar question (or really, the multi-million dollar question)[98] is: what is enough, i.e., what are the "reasonable" measures a company must take to hold onto its intellectual property? On a motion to dismiss where courts evaluate the case on the pleadings,[99] courts have found reasonable efforts exist if the company alleges it: (1) restricts access to the information to only persons on a need-to-know basis, such as "top executives"; (2) requires that the employees sign confidentiality agreements before receiving access to trade secrets; and (3) requires third parties to sign non-disclosure agreements before receipt.[100] Some courts do not even consider the third factor at the early pleading stage and find it is "reasonable" if a company stores the information in a protected location and requires employees to sign confidentiality agreements prior to access.[101]

Overall, it is clear that courts analyze the specific facts of each case in determining whether or not the information is a trade secret and what reasonable measures the owner has taken to protect it. But, courts vary in their analysis of which factors, if any, are more important than others, which makes it difficult —

[95] Westrock Co. & Victory Packaging, LP v. Dillon, No. 21-CV-05388, 2021 WL 6064038, at *9 (N.D. Ill. Dec. 22, 2021).
[96] *Id.* at *12.
[97] *Id.*; Zeigler Auto Grp. II, Inc. v. Chavez, No. 19-CV-02748, 2020 WL 231087, at *4 (N.D. Ill. Jan. 15, 2020) (finding that a former employer acted reasonably when it terminated employees' access to its systems within one to two days of resignation).
[98] Damages have been awarded in the multi-million dollar range in trade secret misappropriation cases. Evan M. Rothstein et al., *Trade Secret Litigation Boom Continues*, ARNOLD PORTER (Feb. 2021), https://www.arnoldporter.com/-/media/files/perspectives/publications/2021/02/trade-secret-litigation-boom-continues.pdf.
99 *See* Cooper v. Pickett, 137 F.3d 616, 622 (9th Cir.1998) ("In ruling on a motion to dismiss, a district court generally 'may not consider any material beyond the pleadings.'")
[100] Upstrem, Inc. v. BHFO, Inc., No. 20-CV-2160 JLS (DEB), 2021 WL 2038324, at *5 (S.D. Cal. May 21, 2021).
[101] VibrantCare Rehab., Inc. v. Deol, No. 2:20-CV-00791-MCE-AC, 2021 WL 1614692, at *3 (E.D. Cal. Apr. 26, 2021); Farmers Ins. Exch. v. Steele Ins. Agency, Inc., No. 2:13-CV-00784-MCE-DAD, 2013 WL 3872950 at *15-16 (E.D. Cal. July 25, 2013); Cutera, Inc. v. Lutronic Aesthetics, Inc., 444 F. Supp. 3d 1198, 1206-07 (E.D. Cal. 2020).

if not impossible — to identify the measures every company must take to protect its trade secrets. With that said, it is clear that a company must undertake multiple measures for its protective efforts to be deemed "reasonable," and no one action is enough.[102] However, in today's digital era, with an increasing number of employees working remotely, the common steps that previously protected trade secrets may now prove insufficient.

III. THE DIGITAL AND WORK-FROM-HOME REVOLUTION

We are living in a "digital revolution" — so described because of how the internet and other digital technology are changing the way we live, communicate, and work.[103] Specifically, as relevant here, the digital boom has allowed a sharp increase in the amount of remote work and the amount of intangible property.

A. INCREASE IN REMOTE WORK

Prior to the pandemic and the stay-at-home orders, twenty-three percent of U.S. workers were teleworking.[104] More jobs could have been done from home at the time, but many employers required their employees to come into the office

---

[102] ExpertConnect, L.L.C. v. Fowler, No. 18 Civ. 4828 (LGS), 2019 WL 3004161, at *4 (S.D.N.Y. July 10, 2019); *see also* Syntel Sterling Best Shores Mauritius Ltd. v. Trizetto Grp., Inc., No. 15-CV-211 (LGS) (RLE), 2016 WL 5338550, at *6 (S.D.N.Y. Sept. 23, 2016) ("Defendants have alleged that they have taken reasonable measures to keep the information secret by making those who use it subject to confidentiality provisions and limitations, and only making it accessible through strictly controlled servers ....."); Albert S. Smyth Co. v. Motes, No. CV CCB-17-677, 2018 WL 3635024, at *3 (D. Md. July 31, 2018) ("[Plaintiff] did take steps to protect its records. Its employees were prohibited from disclosing 'company information and property,' and it stored its business records on encrypted servers protected by firewalls to which only a handful of employees were granted access."); Power Home Solar, LLC v. Sigora Solar, LLC, No. 20 CVS 7165, 2021 WL 2530984, at *14 (N.C. Super. Ct. June 18, 2021) (finding allegations that plaintiff "limited access to the trade secret information to certain employees and required employees to sign nondisclosure agreements before gaining access to the trade secret information" were sufficient under Rule 12 to plead that it took reasonable efforts to maintain the secrecy of trade secrets).

[103] Chris Smith, *10 mind-blowing facts about the digital revolution*, KNOWTECHIE (May 11, 2022), https://knowtechie.com/10-mind-blowing-facts-about-the-digital-revolution/.

[104] Kim Parker et al., *Covid-19 Pandemic Continues to Reshape Work in America*, PEW RSCH. CTR. (Feb. 16, 2022), https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america/ (providing annual data about teleworking for jobs that can be done from home).

even if teleworking was possible, and some employees chose to work in an office even if they were permitted to work remotely.[105] But, when the coronavirus outbreak occurred in 2020, the percentage of remote employees jumped up from twenty-three percent to seventy-one percent.[106] In the past year, the number of employees working from home has declined slightly, but almost sixty percent of employees whose jobs can be done remotely are still working from home today.[107] Some of the increase in work-from-home numbers is due to the employees' choice, with most remote workers stating they are working from home because it is their preference or for personal reasons, while the remainder report that they have no other choice because their workplace is closed or no longer available to them.[108]

There are certainly benefits to companies allowing their employees to work from home. For one, they can keep or recruit more talent; thirty-two percent of workers stated they would quit their jobs if their employer forced them to return to working inside an office. [109] Indeed, surveys show that those working from home are twenty-two percent happier than those who are not.[110] Allowing work-from-home options also cuts down on commute time, travel time, expenses, and also increases productivity.[111] The increase in remote work arrangements has been described as the "largest societal change in America since the end of World War II"[112] and is expected to continue to grow in 2023 and beyond.[113]

---

[105] Fifty-six percent of the workforce holds a job that is compatible or partially compatible with remote work. *Work-at-Home After Covid-19 – Our Forecast*, GLOB. WORKPLACE ANALYTICS, https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast (last visited Oct. 9, 2022); Kim Parker et al., *How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work*, PEW RSCH. CTR. (Dec. 9, 2020), https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/.

[106] Parker et al., *supra* note 104.

[107] *Id.*

[108] *Id.*

[109] *Statistics on Remote Workers That Will Surprise You*, APOLLO TECH. (Dec. 2, 2022), https://www.apollotechnical.com/statistics-on-remote-workers/.

[110] *Id.*

[111] *Id.* Not all managers agree that productivity has increased. "22.5% of survey managers said productivity had decreased compared to 32.2% of hiring managers that said productivity has increased since their employees started working from home in 2020." *Id.*

[112] Bryan Robinson, *Remote Work Is Here to Stay and Will Increase Into 2023, Experts Say*, FORBES (Feb. 1, 2022, 6:24 AM), https://www.forbes.com/sites/bryanrobinson/2022/02/01/remote-work-is-here-to-stay-and-will-increase-into-2023-experts-say/?sh=cc8a53920a6c.

[113] *Work-at-Home After Covid-19 – Our Forecast*, *supra* note 105.

B. INCREASE IN AMOUNT AND VALUE OF INTANGIBLE PROPERTY

In the past, the value of a company was primarily based on its tangible assets, namely its land, equipment, inventory, stocks, and bonds.[114] A company's intangible property, such as its brand name, intellectual property, goodwill, reputation, and licenses, constituted only a small percentage of its value.[115] Today, intangible property comprises ninety percent of the value of S&P 500 companies.[116] In total, intangible property is approximated to be worth $21 trillion for all United States companies.[117] Such intangibles are becoming more valuable than the company's property and equipment, and this is particularly true for trade secrets, as studies suggest that businesses of all sizes consider trade secrets to be as important, if not more important, than other forms of intellectual property.[118]

IV. THE ISSUE: COMPANIES AND COURTS ARE NOT ADAPTING TO THE CHANGES

Work rules and case law have not kept pace with the changes occurring in today's dynamic digital and remote work transformation. These changes should shape how companies operate and protect their information and how courts require them to do so.

---

[114] Bruce Berman, *Latest Data Show That Intangible Assets Comprise 90% of the Value of the S&P 500 Companies*, IP CLOSEUP (Jan. 19, 2021), https://ipcloseup.com/2021/01/19/latest-data-show-that-intangible-assets-comprise-90-of-the-value-of-the-sp-500-companies/#:~:text=According%20to%20long%2Dtime%20purveyor,of%20the%20Index's%20company%20value.

[115] *Id.; see also* Will Kenton, *What Are Intangible Assets? Examples and How to Value*, INVESTOPEDIA, https://www.investopedia.com/terms/i/intangibleasset.asp (last updated Mar. 20, 2022) ("An intangible asset is an asset that is not physical in nature. Goodwill, brand recognition and intellectual property, such as patents, trademarks, and copyrights, are all intangible assets.").

[116] Berman, *supra* note 114.

[117] *Id.*

[118] John Hull, *Protecting trade secrets: how organizations can meet the challenge of taking 'reasonable steps'*, WIPO MAG.(Oct. 2019), https://www.wipo.int/wipo_magazine/en/2019/05/article_0006.html.

A. SEEMINGLY "REASONABLE MEASURES" NOT ANALYZED BY COURTS

While this Article has detailed the factors most commonly analyzed by courts in a reasonableness analysis,[119] this author believes additional issues should be considered just as often in today's digital era.

1. Employee Training

Some courts have identified the training of employees as something a company can do to make its efforts more reasonable. For example, one court found that a company took reasonable measures to keep its information confidential by "requiring employees to use 'multifactor sign-ons' and to undergo 'extensive training [and] regular training throughout the year[] about document control [and] about sensitivity to the information that [they] have access to and [that they are] responsible for.'"[120] But, another court held that a company's failure to provide formal training to its employees on how to treat confidential information does not mean the information loses protection, provided the company has in place formal policies on how to handle that information.[121] No court seems to require initial or updated training which would teach and remind the employees on security protocols and the protection of intellectual property in the "reasonableness" analysis. This seems counterintuitive. Logically, even if employees are informed of trade secrets and company policies when they join the company, they will likely not remember that information in perpetuity, especially considering the changing nature of one's work life and the likeliness that the trade secret information can grow or evolve.

Moreover, while many companies (hopefully) instruct their employees to detect phishing efforts, to not share their passwords, to keep family members off of work devices, to secure their Wi-Fi, and to protect company data, the problem is, that many employees may not know what they need to protect. Often there is nothing physical that the company can show its employee when explaining what needs to be protected.[122] Employees may not know, for example, that a company

---

[119] *See supra* Section II.C (discussing the factors federal courts assess when determining whether a trade secret owner has used "reasonable" efforts to protect its secret).

[120] Arthrex, Inc. v. Hilton, No. 2:21-CV-850-JLB-NPM, 2022 WL 685496, at *9 (M.D. Fla. Mar. 8, 2022).

[121] Workplace Techs. Rsch., Inc. v. Project Mgmt. Inst., Inc., No.: 18CV1927 JM (MSB), 2021 WL 4895977, at *23 (S.D. Cal. Oct 20, 2021).

122 *See* Avery Dennison Corp. v. Allendale Mut. Ins. Co., 47 F. App'x 481, 482 (9th Cir. 2002) (noting "tangible property" is "[t]hat which may be felt or touched, and is necessarily corporeal" and finding "trade secrets are not tangible property with intrinsic value" (citation omitted)).

considers its software code to be proprietary,[123] and without instruction, employees may not see an issue with sharing certain information with a partner, friend, or roommate while working from home, not knowing that doing so could destroy the trade secret's proprietary nature.[124] Therefore, both initial and recurring employee training should be considered in the analysis of "reasonable measures."

2. Increased Cybersecurity

The next issue to consider is a company's level of security to avoid cybercrime. Hacking and cybercrime are on the rise, with remote workers being an increasingly popular target for cybercriminals today.[125] Indeed, while "misappropriation" of trade secrets may have more commonly occurred via actual theft of physical documents in the past, now, information can be more easily stolen remotely via a digital breach.[126] Given this, employers should train their employees to detect phishing, i.e., the use of fraudulent emails or websites to extract data from computer users for purposes of identity or data theft.[127] Employees also should be informed on how to protect their information by using

---

[123] *See generally* Oliver v. Johanson, 357 F. Supp. 3d 758 (W.D. Ark. 2018) (finding methodology embedded in software code was protectable trade secret).

[124] Shannon T. Murphy, *Protecting Trade Secrets In The New Normal: 10 Questions Companies Need to Address in a Work-From-Home Environment*, LEXOLOGY (May 20, 2020), https://www.lexology.com/library/detail.aspx?g=c61c5e13-c90f-4153-b80d-4bea73d682d9 (reporting that employees do not realize "the breadth of information the company has that constitutes valuable 'trade secrets' . . .").

[125] Rebekah Carter, *The Ultimate List of Hacking Statistics for 2023,* FINDSTACK, https://findstack.com/resources/hacking-statistics/ (last updated Sept. 6, 2022).

[126] Reports of ransomware attacks increased over 3000% from 171,000 in 2019/2020 to more than 5.5 million in 2020/2121. Richard Andreae, *Cybercrime is on the rise, is your business prepared?*, OPEN ACCESS GOVERNMENT (Dec. 7, 2022), https://www.openaccessgovernment.org/cybercrime-is-on-the-rise-is-your-business-prepared/143070/#:~:text=As%20technology%20advances%20and%20our,opportunities%20present%20themselves%20to%20cybercriminals.

[127] Adam Hayes, *Phishing: What it is And How to Protect Yourself*, INVESTOPEDIA, https://www.investopedia.com/terms/p/phishing.asp#:~:text=What%20Is%20Phishing%3F,to%20represent%20a%20legitimate%20firm (last updated July 26, 2022).

up-to-date software and strong password protection on company devices.[128] But studies show that such training is being neglected.[129]

In turn, courts need to require companies to do so if they want to own trade secrets. But, it appears that courts have yet to find that failing to take any of these steps constitutes a failure to protect one's trade secret information. With phishing attacks at an all-time high in 2022,[130] it would not be surprising (and in fact would be logical) if courts begin to consider a company's level of digital security in evaluating "reasonableness."

3. Ensuring a Secure and Private Workspace

Finally, although phone calls may seem like a thing of the past,[131] phone call policies should be considered in evaluating a company's reasonable efforts to protect its information. Picture this: an employee receives a call from their boss to discuss a customer list. The boss asks the employee to go through the list on the phone, reading the customer's name and detailing the company's efforts to contact or maintain that customer as a client. The company, as it should, considers this valuable customer list a trade secret.[132] But what if the employee reads this list out loud while working in a shared office space?[133] What if the employee is working from home while their roommate works from the next room and can hear every word they say, and then the roommate uses that list to

---

[128] *How to Recognize and Avoid Phishing Scams*, F.T.C., https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams#protect (last visited Nov. 7, 2022).

[129] *Phishing Awareness Training Neglect Comes Back to Haunt Businesses*, ID AGENT (July 29, 2021), https://www.idagent.com/blog/phishing-awareness-training-neglect-comes-back-to-haunt-businesses/.

[130] *Phishing reaches all-time high in early 2022*, HELP NET SEC. (June 15, 2022), https://www.helpnetsecurity.com/2022/06/15/2022-total-phishing-attacks/.

[131] One article reports that thirty-one percent of those surveyed reported that they do not like talking on a phone, and a similar percentage finds phone calls intrusive and prefers other methods of communication. Thomas von Ahn, *No One Answers the Phone: Why the Decline of Phone Calls Matters*, VIRAL SOLUTIONS (Jan. 17, 2022), https://viralsolutions.net/no-one-answers-the-phone/#h-why-no-one-answers-the-phone-these-days.

[132] *See, e.g.,* Marina Dist. Dev. Co. v. AC Ocean Walk, LLC, No. 22-CV-01592-GMN-BNW, 2020 WL 5502160, at *3 (D. Nev. Sept. 10, 2020) ("Customer lists are generally regarded as trade secrets.").

[133] Currently, there are over 1 million people in the U.S. who use a coworking space. Abby McCain, *33 Captivating Coworking Statistics [2023]: Facts and Trends You Need to Know*, ZIPPIA (Feb. 2, 2023), https://www.zippia.com/advice/coworking-statistics/. One article reports that the number of shared office spaces is projected to increase by more than twenty percent next year. *Why the shared office space trend is good news for landlords*, ENGEL & VÖLKERS, https://www.engelvoelkers.com/en/blog/property-insights/commercial/why-the-shared-office-space-trend-is-good-news-for-landlords/#:~:text=The%20number%20of%20shared%20office,spaces%20in%20the%20USA%20alone (last visited Sept. 28, 2022).

their own advantage?[134] Has the company waived its expectation of privacy in that information due to its employee's actions? Courts evaluate each case on its specific facts, however, speaking a trade secret over the phone to someone not under an agreement of confidentiality could be enough to destroy the trade secret's status.[135]

As to whether the above hypothetical detailing the unwise actions of the employee and boss reading trade secrets over the phone erodes the protections accorded to trade secrets, the answer may be found in the company's other practices. For example, does the company require its employees to sign a confidentiality agreement wherein the employee promises to ensure the secrecy of certain information? If so, the company can argue it did its best to protect its information and the employee and/or the boss acted contrary to company policy.[136] But with the increasing numbers of work-from-home employees, and where companies know that the risk of disclosure may increase with more flexible work arrangements, will the courts find a written confidentiality agreement to be enough? Should companies instead affirmatively require their employees to disclose the details of their workspace and affirm that when outside the office, they can still maintain the company's confidentiality requirements? Likely yes. The majority of Americans find it is generally acceptable to take a cell

---

[134] About one-third of Americans live with a roommate. Richard Fry, *More adults now share their living space, driven in part by parents living with their adult children*, PEW RSCH. CTR. (Jan. 31, 2018), https://www.pewresearch.org/fact-tank/2018/01/31/more-adults-now-share-their-living-space-driven-in-part-by-parents-living-with-their-adult-children/.

[135] *See, e.g.,* Subscriber Holdings, LLC v. Brightstar Corp., No. 1:19-CV-1991-TWT, 2021 WL 3926258, at *5 (N.D. Ga. July 28, 2021), *vacated*, No. 21-12985, 2022 WL 18034431 (11th Cir. Dec. 30, 2022). In that case, a company considered an insurance program called Subscriber Assurance a trade secret. The company's sole owner and employee called a potential customer to pitch the idea and, in doing so, discussed the Subscriber Assurance program over the phone before asking the potential customer to sign a non-disclosure agreement. The potential customer then used the Subscriber Assurance program, and the company sued, claiming misappropriation. The court found that because the company's employee/owner disclosed the program via a phone call prior to the execution of the NDA, the information was not a protected trade secret, and the owner had no claim for unlawful use of the information.

[136] In *Art & Cook, Inc. v. Haber*, 416 F. Supp. 3d 191, 197 (E.D.N.Y. 2017), the company asked its employees to sign an employee handbook and non-disclosure agreement, and the employee refused to sign. Yet, the company still provided them access to what it contended were trade secrets. The court found that the company did not take reasonable measures to protect its information.

phone call in a public area, such as on public transportation,[137] and about one-third of Americans live with a roommate.[138] It is easy to imagine a trade secret slipping out in an overheard phone conversation either on the way to the office or while working from home. One can also picture a roommate in a shared work space inadvertently seeing trade secrets displayed on the screen of another while working in a shared work space. While such disclosure may not be intentional, it is important to note that the drafters of the Uniform Trade Secret Act commented that a disclosure of trade secret information through mere "carelessness" can preclude its protection.[139] Without the company taking efforts to mitigate such accidental or negligent disclosures, the company could lose its trade secret protection. And, without courts requiring more effort, there is less incentive for companies to adopt stricter policies for protection.

B. COMPANIES FAIL TO ADAPT

The other issue is that companies are failing to modify and update their security protocols and remote policies to adapt to the digital age.

Even with the rise in the number of employees working from home, thirteen percent of workers surveyed report that they find it difficult to have or acquire the technology and equipment that they need to do their job to work from home.[140] Even more report it is difficult to have an adequate workspace to get the job done.[141] Only twenty to twenty-five percent of companies report they are paying for the cost of their employees' home office equipment.[142] These low-cost reimbursement numbers are incredible because employers are benefitting

---

[137] Lee Rainie & Kathryn Zickuhr, *Chapter 3: When it is acceptable — or not — to use cellphones in public spaces*, PEW RSCH. CTR. (Aug. 26, 2015), https://www.pewresearch.org/internet/2015/08/26/chapter-3-when-it-is-acceptable-or-not-to-use-cellphones-in-public-spaces/.

[138] Fry, *supra* note 134; *see also* CORPORATE COUNSEL'S GUIDE TO INTELLECTUAL PROPERTY § 26.2: CHECKLIST FOR PROTECTING TRADE SECRETS , Westlaw (database updated Sept. 2022) ("There have been highly publicized cases of people overhearing sensitive information from cell phone calls.").

[139] UNIF. TRADE SECRETS ACT § 1 cmt ("[P]ublic disclosure of information through . . . carelessness can preclude protection.").

[140] *See* Parker, *supra* note 105 (noting that among employed adults who are working from home all or most of the time, thirteen percent say that, since the COVID-19 outbreak, it has been very/somewhat difficult "having the technology and equipment they need to do their job").

[141] *See id.* (providing that survey results show that twenty-three percent of people working from home have a very/somewhat difficult time with "having an adequate workspace").

[142] *See* APOLLO TECHNICAL, *supra* note 109 .

from flex working[143] — to the tune of saving about $11,000 per employee due to the reduced cost of office space and other factors[144] — but many companies are not using these savings to improve their employees' work life or ensure the protection of company information.[145]

This naturally means that employees may be working with outdated technology or in an inadequate space. This is problematic because outdated equipment can mean less security, and a frightening survey reports that seventy percent of employees working from home have experienced a cyber threat.[146] The majority of data breaches during the pandemic occurred because the cybercriminals were able to steal an employee's credentials from the business.[147] For those companies who have experienced data breaches, many contend that their employees working from home was a factor in those data breaches and report an overall loss of millions of dollars.[148]

It is simply beneficial and cost-effective for companies to allow their employees to work from home when possible, but at the same time, spend the extra money to ensure each employee's technology and workspace are up to date and secure. But they have not done so. Certainly, it is easier for one to protect tangible property (like inventory or cash) than intangible property (like a business method or prototype).[149] Hiring a security guard to protect a warehouse of inventory is insufficient to protect digitally stored files on an easily hackable computer. Companies must evolve and change with the times and ensure they have adapted to their protocols and behavior to protect all of their property.

---

[143] A flex work model allows employees to work "when, where, and how they need." Madeline Jacobson, *Why Flex Work Is the Future of Work*, BLOOMFIRE (May 27, 2020), https://bloomfire.com/blog/flexible-work-future/.

[144] *See id.* ("Global Workplace Analytics estimates that employers can save over 11,000 dollars per year per employee. The savings are from the lower cost of office space, increased productivity, reduced absenteeism, and less turnover.").

[145] *See* APOLLO TECHNICAL, *supra* note 109.

[146] *See How to Ensure Cybersecurity During Work from Home?*, THREATCOP, https://threatcop.com/blog/cybersecurity-during-work-from-home/#:~:text=According%20to%20IT%20Governance%2C%2070,the%20factor%20in%20data%20breaches (last visited Sept. 5, 2022).

[147] Carter, *supra* note 125.

[148] THREATCOP, *supra* note 146.

[149] Both are considered trade secrets under the DTSA. 18 U.S.C. § 1839(3).

Indeed, at least one survey reports that remote work has led to more data breaches than ever before.[150] This is due to a variety of factors — namely unsecured networks, out-of-date software, employees failing to follow company guidelines, and the increased ability for hackers to trick employees into giving up information or credentials.[151] It should come as no surprise that, correspondingly, the number of trade secret theft cases is also on the rise.[152] Fortunately, this is not an insurmountable problem as it is possible that the increases in data breaches and theft of intellectual property can be tempered through the recommendation below.

V. RECOMMENDATION: A NATIONAL TRADE SECRET REGISTRAR IDENTIFYING REASONABLE EFFORTS

A "reasonableness" standard is difficult to describe, and the evolving standard has led to copious litigation resulting in varying interpretations and applications of the law.[153] And, more than that, the lack of a clear standard makes it impossible to follow. Without straightforward guidelines, and especially in today's fast-changing business environment, companies are left in the dark as to whether they are doing "enough." Indeed, a company could think it is sufficiently protecting its confidential information but then later sue for misappropriation only to have a court determine the company's actions were not reasonable to begin with, leading to the loss of its trade secrets.

In contrast, if a company owns patents, trademarks, or copyrights, it can register them and receive written proof of ownership and increased protection

---

[150] Matt Murray, *How Remote Work is Leading to More Data Breaches Than Ever*, TMC (Jan. 18, 2022), https://www.tmcnet.com/topics/articles/2022/01/18/451216-how-remote-work-leading-more-data-breaches-than.htm.

[151] *Do Remote Workers Increase Your Chance of a Data Breach?*, SONTIQ (Aug.4, 2022), https://www.sontiq.com/resources/remote-work-data-breach/.

[152] Laura B. Brown, *Trends in Trade Secret Litigation and 7 Tips for Employers in the Post-DTSA World*, FISHER PHILLIPS (Mar. 1, 2022), https://www.fisherphillips.com/news-insights/trends-in-trade-secret-litigation-and-7-tips-for-employers-in-the-post-dtsa-world.html#:~:text=Federal%20Trade%20Secret%20Litigation%20is%20on%20the%20Rise&text=In%202021%20alone%2C%201%2C253%20new,into%20the%20federal%20court%20system (reporting rise in trade secret cases from 2016 to 2022); *see also* John Hull, *supra* note 118 (noting "significant[]"increase in trade secret litigation in the United States).

[153] Reasonableness is a question of fact not only in the trade secret context, but throughout other areas of law as well. *See, e.g.*, Margolies v. Deason, 464 F.3d 547, 553 (5th Cir. 2006) (citation omitted) ("Ordinarily, what constitutes reasonable diligence to discover fraud is a question of fact for the jury."); Vera v. Rodriguez, No. CV 16-491 SCY/KBM, 2018 WL 327236, at *10 (D.N.M. Jan. 8, 2018) (analyzing reasonableness of a police officer's actions and finding "reasonableness is most often a question of fact for the jury").

in court. While registration is not required, it is helpful. For example, the use of a trademark in association with goods or services, even without registering the mark, provides the user with common law rights enforceable in the specific geographic area in which it uses the mark.[154] The owner of a common law mark, however, must prove ownership via use, which requires the user to compile and provide evidence that it has used the mark in connection with things like advertising, services, goods, and billing.[155] On the other hand, a registered trademark provides the owner with a presumption of ownership and of the exclusive right to use the mark in commerce.[156] Similarly, there are benefits to copyright registration. A copyright is automatically placed on a sufficiently original work, and the creator has rights even without a copyright registration.[157] But, a copyright registration (if the work is registered within five years of publication of the work) provides the owner with a presumption of validity of the copyright.[158] Finally, the patent system operates under a "first-to-file" system, meaning an inventor who wants to protect their invention must file a patent

[154] Schwartz, *supra* note 38. Less notably but still important to some registrants, the owner of registered copyrights and trademarks can participate in the U.S. Customs and Border Protection program ("CBP"). This protection allows the CBP to seize and detain imported goods that violate intellectual property rights in the United States. *How to Obtain Border Enforcement of Trademarks and Copyrights*, U.S. CUSTOMS & BORDER PROT., https://iprr.cbp.gov/s/ (last visited Sept. 5, 2022).

[155] Schwartz, *supra* note 38.

[156] 15 U.S.C. § 1115. This does not mean the mark is impervious to attack. A third party can still argue the mark was obtained fraudulently, abandoned, or raise other defenses. 15 U.S.C. § 1115(b); *see also Why register your trademark?,* USPTO, https://www.uspto.gov/trademarks/basics/why-register-your-trademark (last visited Oct. 11, 2022) (providing a list of benefits that come with trademark registration).

[157] See *Copyright in General*, U.S. COPYRIGHT OFF., https://copyright.gov/help/faq/faq-general.html (last visited Mar. 8, 2023) ("In general registration is voluntary. Copyright exists from the moment the work is created.").

[158] 17 U.S.C. § 410(c). Moreover, one cannot file a lawsuit for copyright infringement if he or she does not have a copyright registration. 17 U.S.C. § 411(a). Another benefit of registration is it provides more options for recovering damages. When a copyright is registered prior to any infringement or within three months of publication of the work, a copyright owner can pursue statutory damages, as opposed to simply actual damages. 17 U.S.C. § 412. Statutory damages range from $750 to $30,000 "as the court considers just" and can vary even further to $200 for innocent infringers to $150,000 for willful infringers. 17 U.S.C. § 504(c).

application and receive a patent from the United States Patent and Trademark Office ("USPTO") before they have any protection under the law.[159]

Why should it be any different for the fourth category of intellectual property — trade secrets? Like with other forms of intellectual property, it is logical that the owner of a trade secret should be entitled to more benefits, or at least an easier time of proving entitlement to protection, by registering with a national board. This Article does not suggest that each company must be required to register its trade secrets; of course, publicly identifying exactly what one is trying to protect could negate the point of protecting it.[160] Instead, each company should be encouraged to disclose how it is protecting its trade secrets: in other words, register and document its "reasonable" actions.

A. A NATIONAL REGISTRAR AND ITS CRITERIA

To make this solution a reality, a trade secret board, similar to the USPTO,[161] should be formed; it could be called the "National Trade Secret Registrar" (the "Registrar"). Like the USPTO, the Registrar would be an agency of the United States, subject to the policy direction of the Department of Commerce, but charged with responsibility for its own management and administration and with independent control of its operations.[162]

That Registrar can create and publish a set of standards that companies may use to protect their trade secrets. These standards should include the following elements, which have been found to be reasonable by many courts, and even elements that are not:

1. Upon hire, all employees who may receive or have access to trade secrets must sign agreements attesting that they understand the company has proprietary information that will be shared with them,

---

[159] *First-to-File Rule for Patent Applications*, JUSTIA, https://www.justia.com/intellectual-property/patents/first-to-file-rule/ (last updated Oct. 2022).

[160] Such an idea, however, is not impossible. There could be a national board that reviews trade secrets privately, without disclosure to the public, to determine if they are worthy of protection. This would be similar to how courts often review information *in camera* to determine whether such information sufficiently constitutes trade secrets. *See In re* Remington Arms Co., Inc., 952 F.2d 1029, 1033 (8th Cir. 1991) ("[T]he district court should afford [petitioner] the opportunity to make a showing that the disputed documents contain trade secrets. It may (and probably should, given the highly charged relationship that has developed between the parties) examine the documents *in camera* in deciding this threshold question.").

[161] Congress established the USPTO via 35 U.S.C. § 1.

[162] *See* 35 U.S.C. § 1 (explaining establishment of USPTO).

they understand what it is, and that they will undertake efforts to ensure that information remains secret and proprietary. The employees must attest several things, including:

   a. They will ensure their computer set-up, whether at home or in the office, is password protected and that the screen locks when the employees are away from the computer. This requirement should also apply to the employees' phones and to any other device in which trade secrets are accessible.
   b. They will ensure that all phone conversations pertaining to proprietary information will take place in private and not on public transportation, in a ride-share vehicle, or in places where others may overhear the conversations.
   c. If the employees have physical trade secrets in their workspace (i.e., prototypes or printed documents), these will be kept secure and private.

2. Companies must share trade secret information internally only on a need-to-know basis. This also includes ensuring that all trade secrets are removed from each employee's computers, hard drives, and phones when that employee leaves the company.
3. Companies must keep their trade secrets in a protected location, such as a password-protected drive accessible only to those whose access is critical. Companies must also take steps to protect their systems from phishing efforts or data breaches, either via password encryption or through changing the passwords at set intervals.
4. Companies must implement early training to ensure the employees are informed as to which information the companies contend is proprietary and how it may be shared, if at all. This training should also teach the employees how to avoid cybercrime or data breaches by protecting the security of their workspace. Training must be renewed yearly and must include a report on the most common or possible phishing attempts to ensure the employees are kept current and are guarded against such attacks.
5. Companies must provide employees with guidance and rules for remote work (if applicable) and conduct an internal analysis on how

to factor the number and location of remote workers into protecting the information to which the employees have access.

6. Companies must implement guidelines on how their employees may share (if necessary) proprietary information with outside third parties and vendors. This should include clearly marking such information as "CONFIDENTIAL" and ensuring that all third parties who receive said information sign an agreement attesting to their understanding of its proprietary nature.[163]

The Registrar would have the discretion to edit the standards annually or make additions as it sees fit in light of any change in the business culture or case law. Once the Registrar forms and publishes these standards, each company may complete paperwork with the Registrar attesting how the company ensures it is achieving each standard. If the Registrar is satisfied that the company is in compliance, then the Registrar will issue a "Trade Secret Protection" certificate. The certificate will require annual renewal, so the Registrar will send the company a yearly reminder prompting the company to double-check its security precautions and conduct updated employee training. When companies certify they have done so, the Registrar will update and re-issue the certificate. Ownership of this certificate carries with it the presumption that the company has implemented reasonable measures to protect its trade secrets.

B. CAVEATS TO THIS PROPOSAL

First, like most presumptions, this one can be overcome.[164] For example, when facing the presumption in a misappropriation case, an alleged misappropriator could present evidence that the company in fact did not keep up with the Registrar requirements as it had attested or that the company was following the criteria for some but not all information it deemed a trade secret. If the proof was sufficient, the company would lose its presumption of reasonableness.

---

[163] Many courts have form protective orders that require any receiver of the litigant's confidential information to sign an acknowledgment of the protective order and agreement to be bound. A similar form could be required for the sharing of any trade secret information. *See*, *e.g.*, *Model Protective Orders*, UNITED STATES DISTRICT COURT, N. DISTRICT OF CAL., https://www.cand.uscourts.gov/forms/model-protective-orders/ (last visited Nov. 12, 2022) (showing an example of a model protective order for one federal court).

[164] This is not unknown in the intellectual property world. For example, an issued patent is presumed valid, but that presumption can be overcome by clear and convincing evidence. Microsoft Corp. v. i4i Ltd. P'ship, 564 U.S. 91, 95 (2011).

Second, a company would not be required to achieve this registration status for its actions to be deemed reasonable under the DTSA. Because every company is different, this Article does not propose a litmus test requirement mandating registration by every trade secret owner. Some companies may find it is not worth the burden to complete this registration if they determine the cost of the steps or of registration exceeds the value of the trade secrets. Although registration is not mandatory, the standards will be available online for public view, so all companies can review the guidance on what is deemed "reasonable measures."

This standard of voluntary compliance mirrors that for other intellectual property like trademarks. Under trademark law, simply because a company's trademarks are not registered does not mean the company is out of luck if its intellectual property is infringed upon.[165] But, lack of registration does mean that the company will have a more difficult time meeting its burden to prove a valid trademark.[166] Its "reasonable measures" registration via the Registrar is no different; it is not required, but helpful.

C. POSSIBLE CRITIQUES OF THIS PROPOSAL

Critics may argue that this proposal is unnecessary and a redundant expense; after all, we have courts to determine whether a company is acting reasonably. This point is well-taken, but as this Article points out, case law does not provide clear guidance on what are and are not reasonable measures to protect trade secrets, and many companies may not understand what is required. Moreover, like the cost of the USPTO, the cost of the Registrar could be covered, at least in part, by requiring companies to pay a fee to receive a registration.[167] Finally, trade secret misappropriation cases will likely spend less time in court if

---

[165] Schwartz, *supra* note 38.

[166] *See* OTR Wheel Eng'g, Inc. v. W. Worldwide Servs., Inc., 897 F.3d 1008, 1024–25 (9th Cir. 2018) (citations omitted) ("[R]egistration only provides a presumption of validity, shifting the burden to the defendant to rebut either distinctiveness or non-functionality.").

[167] *Fiscal Year 2022 Congressional Justification*, USPTO 3 (May 2021), https://www.uspto.gov/sites/default/files/documents/fy22pbr.pdf ("The USPTO is a demand-driven, fee-funded, performance-based organization .....").

companies are provided a presumption of reasonableness, and thus this proposal will save on judicial resources in that regard.[168]

Critics may also argue that this proposal would impose government oversight onto a company that may want to stay out of the spotlight, forcing the company to choose between involving itself with the national registrar or risk having to defend itself in court should its information ever be misappropriated. However, this is true as to all other forms of intellectual property; trade secrets should be no different.

Another possible criticism of this proposal is that it could encourage companies to go too far to protect their trade secrets. Some companies have implemented apps or websites that collect information from remote employees through facial recognition, keystroke logging, and the tracking of work time with screenshots and website monitoring.[169] It is plausible that some companies could monitor their employees' every move in a guised attempt to protect their proprietary information. Hopefully, such a scenario is unlikely as companies should keep the best interests of their employees and their valuable trade secrets at the forefront of their concerns.

A final critique of this proposal is that its adoption could open up non-compliant companies to theft. For example, a potential misappropriator could review the publicly-available registrations of compliance to see which companies are not listed and, thus determine which companies are vulnerable to trade secret theft. The likelihood of this scenario seems slim, as it is not easy for just anyone to infiltrate a company to steal its trade secrets. Moreover, because the registering companies would not be required to list the actual trade secrets, someone reviewing the registration would not be aware of the identity or value of the trade secret without being part of the company.

D. BENEFITS OF THIS PROPOSAL

[168] *See* Anne L. Alstott et. al., *Psychological Parenthood*, 106 MINN. L. REV. 2363, 2433 (2022) (opining in a different context that a presumption provides legal benefits of "less litigation" and "greater predictability"); *see also* Stanley v. Illinois, 405 U.S. 645, 656–57 (1972) ("Procedure by presumption is always cheaper and easier than individualized determination.").

[169] Teramind, a provider of employee-monitoring software, reported that "before the pandemic, about 70% of its sales came from companies concerned about security and 30% from those focused on worker productivity. That balance has since flipped." Don Lee, *Is your company secretly monitoring your work at home?*, YORK DISPATCH (Nov. 24, 2021, 12:23 PM), https://www.yorkdispatch.com/story/money/business/2021/11/24/company-secretly-monitoring-work-home/49430895/.

As mentioned, it is expected that this proposal will decrease the amount of time companies spend in court defending their actions.[170] This proposal will also reduce the number and scope of lawsuits, which in turn means that companies pay less in legal fees and the already taxed court system has fewer cases on the docket.[171]

Another benefit to this proposal is that it will make it simpler (and possibly more likely) for companies to allow their employees to work from home. If companies are currently hesitant to allow their employees to work from home due to the security risks, then a national register and simple checklist to follow will put minds at ease. Many companies may want to give their employees the benefit of working from home where possible but are hesitant to do so because they recognize that they have insufficient security, protocols, or training. While adding this extra protection will certainly cost time and money, the good news is that those same companies should save money on various in-office services — like rent, utilities, and cleaning services — while more employees work from home.[172]

Another benefit is that registration could serve as a deterrent to misappropriation. Trademark and copyright registrations dissuade those who are considering adopting similar intellectual property.[173] A publicly available and

---

[170] A report from 2019 estimated the average cost to litigate a trade secret lawsuit was about $4.1 million, depending on the value of the trade secrets and the financial risk. *Trade secret litigation 101*, THOMSON REUTERS (Nov. 23, 2022), https://legal.thomsonreuters.com/blog/trade-secret-litigation-101/#:~:text=Trade%20secret%20litigation%20can%20be,%2425%20million%20was%20%244.1%20million.

[171] Federal courts in (at least) Arizona and California have reported being overburdened. *See* Ryan Knappenberger, *Judge tells lawmakers Arizona federal courts are overloaded, overworked*, CRONKITE NEWS (Feb. 24, 2021), https://cronkitenews.azpbs.org/2021/02/24/judge-tells-lawmakers-arizona-federal-courts-are-overloaded-overworked/ ("U.S. District Judge Diane Humetewa was joined by other judges and law professors who called on Congress to fill vacancies and consider reforms for the justice system to streamline operations and share some of the load.").

[172] Baruch Silvermann, *Does Working From Home Save Companies Money?*, BUSINESS.COM, https://www.business.com/articles/working-from-home-save-money/ (last updated Mar. 6, 2023).

[173] Aaron Haar et al., *Why Register My Trademark? The Benefits of Trademark Registration*, JDSUPRA (Sept. 17, 2009), https://www.jdsupra.com/legalnews/why-register-my-trademark-the-benefits-58054/; Edward A. Haman, *The term "all rights reserved" explained*, LEGALZOOM,

easily searchable list of companies who have received a certificate of reasonableness may deter misappropriators from attempting to steal trade secrets from that company. Such a list will also give companies more peace of mind to know they are on the right track to protect their valuable material.

Finally, this proposal allows a company to better protect its trade secrets, and by doing so, a company increases its value and makes itself more marketable to investors, employees, and business partners.[174] With a certificate of reasonableness in hand, companies will finally have a tangible asset to point to in order to identify its intangible assets and therefore should be able to confidently say that they own protectable assets. This benefit is expected to increase the present and future value of the companies.[175]

VI. CONCLUSION

As the great Bob Dylan once sang, "the times they are a-changin'."[176] The law must change with the times, and the creation of a national and objective Registrar can put all companies and courts on the same page. Adopting this proposal reduces the guesswork that companies must do to protect their most valuable trade secrets. No longer will companies fail to implement important trainings, reminders, or confidentiality agreements — mistakes that could lead to the loss of trade secrets. This proposal can assist companies in increasing the value and importance of their intellectual property, the security of the workplace, and the happiness of their employees. A win, win for everyone.

https://www.legalzoom.com/articles/the-term-all-rights-reserved-explained (last updated Dec. 5, 2022).

[174] "[I]ntellectual property can be far more valuable than a physical asset. It often provides a competitive advantage over other entities, making it particularly guarded and protected by those that own it." *Why Intellectual Property Is So Valuable to Businesses*, FELDMAN & FELDMAN (June 17, 2020), https://feldman.law/news/why-intellectual-property-is-so-valuable-to-businesses/.

[175] *Valuing Intellectual Property Assets,* WIPO*,* https://www.wipo.int/sme/en/ip-valuation.html (last visited Sept. 29, 2022) (proposing that to value an intellectual property asset, the asset should be "identifiable" and there should be "tangible evidence" of its existence).

[176] BOB DYLAN, THE TIMES THEY ARE A-CHANGIN' (Columbia Records 1964).