MITCHELL | HAMLINE
School of Law

December 22, 2015

The Honorable Charles E. Grassley
Chairman
Judiciary Committee
United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Patrick J. Leahy
Ranking Member
Judiciary Committee
United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Grassley and Ranking Member Leahy:

This letter is submitted by the undersigned, Professor Sharon K. Sandeen, to respond to the questions Senator Sheldon Whitehouse posed during the December 2, 2015 hearing, "Protecting Trade Secrets: the Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy This Harm" and to expand upon the letter in opposition to the Defend Trade Secret Act of 2015 (the DTSA) that was signed by myself and 41 other law professors.[1]

Two points must be stressed at the outset. First, it appears that the focus of most Senators' concerns was on the ability of large U.S. companies to remain competitive with foreign companies, the fear being that without a federal civil trade secret law foreign companies will come to possess U.S.-generated trade secrets and use them to compete against U.S. companies. While I share this concern, Congress should also be concerned about the interests of U.S.-based individuals and companies (including entrepreneurs and small and medium-sized enterprises

[1] *See* Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326), dated November 17, 2015, available at: https://cyberlaw.stanford.edu/files/blogs/2015%20Professors%20Letter%20in%20Opposition%20to%20DTSA%20FINAL.pdf.

(SMEs)) that wish to build competitive businesses within the U.S. but are often hindered in doing so by the over-assertion of intellectual property (IP) rights, including trade secret rights. Trade secrets laws should not be made so strong that they can be used to quell legitimate competition.

Second, trade secret rights should not be made so strong that they tie-up the free flow of information because (like limited incentives) information and knowledge are essential components of innovation, invention and creativity.[2] Rather, the focus should be on finding the optimal balance between protecting truly "secret" information and allowing other information (including the general skill and knowledge that workers learn on the job, which are not protectable as trade secrets under existing law) to flow freely. I think this balance has largely been achieved under existing state laws due to the "sieve-like" nature of U.S. trade secret rights. I am concerned that this balance will be significantly altered by the DTSA, leading to more litigation[3] and less innovation, competition and labor mobility.

Question 1: In executing a civil seizure order under the Defend Trade Secrets Act ("DTSA"), what degree of force would law enforcement agents be entitled to use? Would law enforcement agents executing the seizure be permitted to knock down doors? Open locked cabinets by force? Should they be authorized to restrain the defendant or sequester staff and employees during the search of a business?

Response: As currently written, the DTSA provides little guidance to law enforcement on how the *ex parte* civil seizure order (hereinafter "seizure order" or "seizure remedy") will be executed and whether and to what extent force may be used during its execution. It is clear, however, that the basis for a seizure order is not the same as it is for a criminal search and seizure order and, thus, a civil seizure order should not be executed in a similar manner. The target of a civil seizure order is not being accused of a crime but, instead, is being sued for a civil wrong for which a variety of remedies are available.

Although the seizure order proposed in the DTSA is often favorably compared to the seizure order that exists under federal trademark law,[4] the "property" to be seized is markedly different, as is the required egregiousness of the underlying behavior.[5] Whereas the similar

---

[2] Alan Hyde, WORKING IN SILICON VALLEY: ECONOMIC AND LEGAL ANALYSIS OF A HIGH-VELOCITY LABOR MARKET (2003) and Alan Hyde, *The Wealth of Shared Information: Silicon Valley's High-Velocity Labor Market, Endogenous Growth, and the Law of Trade Secrets, available at* http://andromeda.rutgers.edu/~hyde/WEALTH.htm; *see also,* Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. Rev. 575, 585-92 (1999) (describing the value of knowledge spillovers in the development and growth of Silicon Valley).

[3] *See* Sharon K. Sandeen, *The DTSA: The Litigator's Full-Employment Act*, 72 Wash. & Lee l. Rev. Online 308 (2015).

[4] 15 U.S.C. § 1116(d).

[5] For a more in depth analysis of the civil seizure remedy, *see* Eric Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, 72 Wash. & Lee L. Rev. Online 284 (2015).

provisions of trademark law focus on trademark counterfeiters, no attempt is made in the seizure provisions of the DTSA to differentiate between egregious and minor instances of trade secret misappropriation. Moreover, in the trademark context, physical goods are seized which clearly bear infringing trademarks. Once seized, these goods can be stored much like they would be maintained by a wholesaler until such time as they are either released to the defendant for resale because they are not, in fact, counterfeit goods, or destroyed if they are counterfeit goods.

The execution of a seizure order in a trade secret case will not be so precise and orderly because the putative trade secrets will not be as easy to identify as goods bearing trademarks. Rather, execution of a seizure order in a trade secret case is likely to require law enforcement personnel, unaccompanied by any representative of the applicant,[6] to sift through reams of physical and digital records to find the proverbial "needle in a haystack." Unless the alleged trade secrets can be easily identified and segregated from other information and data, the seizure of non-trade secret information and trade secrets that are owned by the defendant is likely to occur in the process.[7]

The seizure provision of the DTSA requires that service of any order "shall be made by a Federal Law enforcement officer, or may be made by a State or local law enforcement officer, who upon making service, shall carry out the seizure under the order to be executed."[8] Without further specification, this undoubtedly means that a team of uniformed officers will descend upon the target individual's home or business and effectively shut down business operations while the physical premises and electronic equipment can be searched. The draft legislation does not specify what will happen in the case of a recalcitrant defendant that refuses to grant access to the premises or computer systems.

In contrast to the DTSA, the original "Anton Piller Order" that I referred to in my testimony was limited with respect to how it could be executed. As Lord Denning explained in the case of *Anton Piller KG v. Manufacturing Processes Limited*:

> But the Order sought in this case is not a search warrant. It does not authorise the Plaintiffs' Solicitors or anyone else to enter the Defendant's premises against his will. It does not authorise the breaking down of any doors, nor the slipping in by a back door, nor getting in by an open door or window. It only authorises entry and

[6] S. 1890. The Defend Trade Secrets Act of 2015 (hereinafter DTSA), §2(a) ("(b)(2)(B)(iii)(I)").
[7] *See* Goldman, *supra* note 5, at 290 (noting that trade secret information is often commingled with other, non-confidential information); *see also* David Post, *A Misguided Attempt to "Defend Trade Secrets*," Washington Post, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/02/and-we-need-stronger-protection-for-trade-secrets-because (Dec. 2, 2015) (explaining that "the distinction between information that is protected and information that is not protected" under trade secrets law "is usually in dispute and quite difficult to discern").
[8] DTSA § 2(a), ("(b)(2)(E)").

> inspection by the permission of the Defendants. The Plaintiff must get the Defendant's permission.[9]

Senator Whitehouse's question and the foregoing quote raise the very important issue whether seizure orders should be executed like criminal search and seizure orders. Since it is contended by the proponents of the DTSA that seizure orders will be difficult to obtain, it is also worth considering whether the limited benefits of such a remedy are worth the potential for errors and abuse.

Question 2: Who should be responsible for sorting through the data and electronic devices seized pursuant to a DTSA civil seizure order? Should courts permit the plaintiff who initiated the suit to search through the seized devices to locate stolen trade secret information? Isn't this role best performed by a disinterested third party appointed by the court?

Response: As currently written, the DTSA requires that any materials seized "shall be taken into custody of the court,"[10] but it does not specify whether or when seized property, including electronic equipment and digital data, will be evaluated and sorted to determine what portion of it constitutes the plaintiff's legitimate trade secrets. To the contrary, it requires that the seized materials be secured from "physical and electronic access during the seizure."[11] This means that no one has the right to access the seized property until the seizure order is lifted or some process for review is mandated by the court. Even if the seizure order is ultimately lifted, the initial hearing on the validity of the order need not be heard for seven days, the practical effect of the order being that a company's business operations may be shut-down for at least a week.

By no means should the plaintiff in a trade secret case be allowed to search the seized information for the simple reason that it may contain the confidential personal information of the defendant's clients, customers and employees, as well as the defendant's own trade secrets and other proprietary information.[12] Instead, if court personnel cannot do so, a special master or other third-party must be retained to review the seized materials. If the seized property includes digital data, this may include an expert in computer forensics. Thus, the expense of storing, evaluating

---

[9] *Anton Piller KG v Manufacturing Processes Ltd & Ors* [1975] EWCA Civ 12, [1976] 1 All ER 779 (8 December 1975). *See also*, UK Parliament. Civil Procedure Act 1997, Section 7. Since *Anton Piller* orders were originally recognized in the United Kingdom, they have been severely criticized by members of the judiciary and others based upon the principle that individuals should not be deprived of their property without due process and concerns about the sanctity of one's home. *See e.g.*, Universal Thermosensors Ltd. v. Hibben [1992] F.S.R. 361, Nicholls V.C.; Columbia Pictures Industries, v. Robinson [1986] F.S.R. 367, Scott J. This includes criticism by the late Sir Hugh Laddie, a highly-respected jurist and IP expert and the person who, as an attorney, advocated for the issuance of the seizure order that was granted in the *Anton Piller* case. Sir Laddie described the remedy that he is credited with inventing as a "Frankenstein's Monster." Obituary of Professor Sir Hugh Laddie, The Telegraph, 03 Dec. 2008, available at http://www.telegraph.co.uk/news/obituaries/3546410/Professor-Sir-Hugh-Laddie.html.

[10] DTSA, § 2(a), ("(b)(2)(D)").

[11] *Id.*

[12] "Searches and seizures of computers and computer data present complex legal questions that, if resolved incorrectly, present a very real threat of massive intrusions into civil liberties." Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 76-77 (1994).

and sorting through the seized information to determine if it contains trade secrets is likely to be extremely high and the DTSA does not specify who will bear those costs.

Equally troubling is the fact that the DTSA contains language that can be interpreted to mean that the scope of any seizure order is not limited to existing legitimate (or even alleged) trade secrets. It states that courts may "issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[13] The terms "propagation" and "dissemination" are not defined in the DTSA, are not terms previously used in connection with trade secret misappropriation and appear to encompass a broader set of behaviors than state trade secret laws. Trade secret misappropriation is defined under the UTSA (and the DTSA) as the wrongful acquisition, disclosure or use of trade secrets.[14] As used in the proposed seizure remedy, the acts that may trigger a seizure of property are not the "threatened disclosure or use" of the alleged trade secrets as required for injunctive relief, but the threatened propagation or dissemination of such information (the act of sharing). Thus, a former employee of a company might be subject to a seizure order if there is a threat that information he holds might be shared with another (e.g., a new employer), even if neither the former employee nor the new employer threaten to publicly disclose or use such information.[15] Furthermore, the property that can be seized could include equipment that can be used for the propagation and dissemination of information, disconnected from the actual trade secrets, such as a computer or smart phone.

Question 3: Testimony offered at the hearing indicated that a civil seizure order issued pursuant to the DTSA could not be used to seize data in the cloud because the DTSA requires that the defendant be in possession of the misappropriated trade secret. Do you agree with this assessment? Isn't a civil plaintiff likely to argue that a defendant possesses the data the defendant stores in the cloud? Doesn't the dictionary definition of "possession," which includes ownership or control, support this argument?

Response: The language of the DTSA is internally inconsistent and therefore confusing. As just noted, it appears to allow for the seizure of "property" that might be used in the propagation and dissemination of trade secrets even if the property itself does not contain the plaintiff's trade secrets. Later, the DTSA specifies a number of conditions for the grant of a seizure order, including that the plaintiff "is likely to succeed in showing that the information is a trade secret"[16] and that "the person against whom seizure would be ordered has possession of the trade

[13] DTSA, § 2(a), ("(b) (2)(A)(i)").
[14] UTSA, § 1(2) and DTSA, § 2(b)(3) ("(5)(A) and (B)").
[15] This is the fact pattern of *Pepsico v. Redmond*, 54 F. 3d1262 (7th Cir. 1995), the case often cited in support of the inevitable disclosure doctrine. Both Mr. Redmond and his new employer (Quaker Oats) readily acknowledged (and agreed to abide by) the ongoing duty Mr. Redmond owed not to disclose or use trade secrets he learned while at Pepsico, but injunctive relief was ordered anyway based upon the argument that Redmond could not separate what he knew about Pepsico from his work with his new employer. Will a seizure remedy be issued based upon the alleged inevitable propagation or dissemination of such secrets?
[16] DTSA, § 2(a) ("(b)(2)(A)(IV)(aa)").

secret."[17] However, while the "matter to be seized" must be described with reasonable particularity, it need not be limited to the alleged trade secrets.[18]

There is nothing in the DTSA that specifically insulates service providers that store information on behalf of a defendant (including cloud storage providers and hard-copy document storage facilities) from being subjected to a seizure order. There is no indication of exactly how electronically stored information will be seized or what it means to be in "possession" of such information. Does "seizing" information that exists in digital form require that it be permanently erased from the computer servers of the person or company against whom a seizure order is issued? What if the information is also stored with a third-party cloud storage provider for back-up purposes; will all copies be seized by law enforcement and stored and sorted by the courts?

While the DTSA provides that "the person against whom seizure would be ordered" must have either "misappropriated the trade secret of the applicant by improper means" or "conspired to use improper means to misappropriate the trade secret of the applicant,"[19] this language does little to insulate cloud storage providers from the reach of a seizure order. To understand why requires consideration of the definition of "misappropriation by improper means," which includes "breach or inducement of a breach of a duty to maintain secrecy."[20] If a cloud storage provider owes a duty of confidentiality to the trade secret owner, it might be subjected to a seizure order if it is shown that it breached its duty and, thereby, "misappropriated the trade secret of the applicant." If no such duty of confidentiality exists (and cloud storage providers are loathe to agree to such a duty), then arguably the trade secrecy of the stored information has been lost, in which case the lawsuit should not be brought in the first place.[21]

The requirement that the person against whom seizure would be ordered must have "conspired to use improper means to misappropriate the trade secret of the applicant" further confuses and complicates the potential reach of any seizure order. If proof of possession of the alleged trade secret by the person against whom the seizure would be ordered is required, what does the conspiracy-prong add to the seizure provision? Usually, a conspiracy claim is included in a statute to punish preliminary behaviors that have not yet resulted in the primary wrongful act. But if the wrongful act of trade secret misappropriation has not yet occurred, how can the person against whom seizure would be ordered possess the alleged trade secrets? Might the conspiracy requirement be used to subject an individual or business, including a cloud storage provider, to a seizure order merely because they possess a misappropriated trade secret? Moreover, who "possesses" the information that is stored with a cloud storage provider: the

[17] DTSA, § 2(a) ("(b)(2)(A)(IV)(cc)").
[18] DTSA, § 2(a) ("(b)(2)(A)(V)").
[19] DTSA, § 2(a) ("(b)(2)(A)(IV)(bb)").
[20] DTSA, § 2(b)(3) ("(6)(A)").
[21] Sharon K. Sandeen, *Lost in the Cloud? Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 Virg. Jour. of L & Tech. (JoLT) 1 (2014).

client, the provider or both? Nothing in the DTSA precludes a court from ordering the seizure of information in defendant's "possession," wherever it might be stored.

Question 4: Are the protections in the DTSA against over seizure a meaningful constraint? Is a court that has found sufficient evidence to grant a civil seizure order likely to later rule that the seizure was wrongful or excessive? If law enforcement agents executing a civil seizure order over seize or act wrongfully would the plaintiff be liable for their actions?

Response: This question raises the very important point of how laws are actually applied in practice and whether the fee shifting provisions of the DTSA, including the damage remedy specified in the seizure provision, are effective in preventing abusive trade secret litigation. The proponents of the DTSA argue that the ability of defendants to obtain an award of attorney's fees in cases of "bad faith" assertion of trade secret claims[22] and damages due to a "wrongful or excessive" seizure[23] are sufficient to deter abusive trade secret litigation. However, as Senator Whitehouse's question suggests, providing a remedy on paper and structuring the remedy so that it can be used effectively are two different things.

Significantly, neither the attorney's fees provision of the DTSA nor the damages provision of the seizure remedy provide defendants with relief based upon the simple fact that they prevailed on the merits in court. Rather, a successful damage claim can only be brought under the seizure provision if it can be shown that the defendant suffered damages "by reason of a wrongful or excessive seizure." A successful claim for attorney's fees requires a showing of "bad faith" on the part of the plaintiff with respect to either: (1) plaintiff's claim of misappropriation; or (2) plaintiff's opposition to a motion to terminate an injunction. It is unclear whether the damage claim for a wrongful or excessive seizure could include attorney's fees and, if so, whether the necessary standard of proof is "bad faith" or "wrongful or excessive."[24]

Further confusing matters, the DTSA does not define "bad faith," "wrongful" or "excessive." It is clear, however, that for a defendant to be awarded a remedy in the form of either attorney's fees or damages, it will have to go to the time, trouble and expense of proving facts beyond merely prevailing in the underlying action. It is also clear that a significant amount of resources will have to be expended before the defendant will even get to the point of claiming attorney's fees and damages, resources that many entrepreneurs, employees and SMEs simply do not possess.

---

[22] DTSA, §2(a) ("(b)(3)(D)").
[23] DTSA, §2(a) ("(b)(2)(G)").
[24] As Eric Goldman notes in a recent article, since explicit reference is made in the DTSA to the analogous provisions of the Trademark Act (15 U.S.C. 1116(d)(11)), the range of potential damages for wrongful or excessive seizures may include attorney's fees (Goldman, *supra* note 4, at 293), but the trademark statute uses a "wrongful" standard whereas the seizure provision uses a "wrongful or excessive" standard. It is not clear if this standard is intended to be easier to prove than the trademark standard and, if so, whether it will apply with respect to attorney's fees expended in conjunction with defending against a seizure order.

The commentary to the UTSA explains that "Section 4 allows a court to award reasonable attorney fees to a prevailing party in specified circumstances as a deterrent to specious claims of misappropriation, to specious efforts by a misappropriator to terminate injunctive relief, and to willful and malicious misappropriation." As an example, the California courts have interpreted "bad faith" to require both proof of "objective speciousness" and "subjective bad faith."[25] This is a very difficult and costly burden to meet and one that falls particularly hard on small businesses that may be victimized by the over-assertion of trade secret rights.

What the required proof will be under the seizure remedy remains to be defined by the federal courts, particularly since the language used is different from the existing "bad faith" language for an award of attorney's fees under the UTSA. As Eric Goldman explained in a recent article:

> With respect to the Seizure Provision's effects, the devil is in details that Congress has not resolved (yet). If the courts interpret the Act to create strict liability for a wrongful seizure and award large damages from lost business opportunities, trade secret owners will be too afraid to use the provision. In contrast, if courts require subjective bad faith to establish a wrongful seizure and narrowly construe the damages from disruption and lost business opportunities, trade secret owners will seek ex parte seizures routinely.[26]

Without more clarity regarding Congressional intent concerning the meaning of "wrongful or excessive," at best, the meaning of the damages provision of the seizure remedy is sure to be highly litigated and, and worst, it will fail in its stated purpose of deterring abusive requests for such relief.

Question 5: Should civil seizure under the DTSA be limited to those instances where a defendant is likely to flee the United States? Should more be done to carve out routine employer-employee disputes from the civil seizure provisions of the DTSA?

Response: I believe that the seizure remedy should be eliminated from the DTSA in its entirety because of its potential for abuse and because the number of cases of egregious trade secret misappropriation involving alleged spies and other acts of wrongful acquisition are small in comparison to the number of cases involving former employees and alleged breaches of a duty of confidence. In this regard, it is interesting to note that at the time that the Economic Espionage Act of 1996 (the EEA) was debated, numerous concerns were expressed about the potential of exposing reputable businesses to criminal prosecution for trade secret misappropriation. At that

[25] Gemini Aluminum Corp. v. California Custom Shapes, Inc., 95 Cal. App. 4th 1249, 1262 (2002).
[26] Goldman, *supra* note 4, at 293.

time, it was agreed by the Clinton Administration that no EEA prosecutions would be brought unless they were first reviewed by the Attorney General of the United States. There should be similar concerns with respect to the use of the seizure provisions of the DTSA against reputable U.S. businesses and employees, particularly where the criminal enforcement tools of the U.S. government can (and should) be brought to bear against the most egregious forms of trade secret misappropriation.

The vast majority of trade secret misappropriation cases in the U.S. do not involve individuals fleeing overseas. A large percentage of them do not even involve legitimate trade secrets or provable acts of misappropriation. Often they involve former employees taking information from a former employer that they were given access to, did not know or have reason to know were trade secrets, or have no intention to disclose or use. These cases can typically be resolved through self-help and education, including informing former employees of their ongoing duties of confidentiality, if any.

In light of the paucity of cases to which the seizure remedy might apply, the argument in favor of the remedy becomes circular. On one hand it is argued that the seizure remedy is necessary to stop egregious behavior that many U.S. companies are facing, but on the other hand it is argued that it will be used infrequently. The critical issue is: How frequently will the remedy be asserted against the typical person (usually a former employee) or U.S.-based company accused of trade secret misappropriation? My concern, and that of other opponents of the DTSA, is that the seizure remedy will be used more frequently against U.S. companies and employees than alleged foreign spies. Further, even if the remedy is sought but not granted, it will impose significant costs on the federal courts. In cases where the remedy is granted but later rescinded, significant costs will also be imposed upon the defendant under circumstances where it cannot recoup such costs unless it can prove that the order was "wrongful" or "excessive."

Senator Whitehouse was correct to note the emotional aspects of trade secret litigation, particularly in the employment context. Although most employers in the U.S. treat their employees as "at-will" so that the obligations that they owe to such employees are limited, they often expect a degree of loyalty that extends well beyond the termination of employment, even in cases where there is no express noncompete or nondisclosure agreement. This is why many trade secret cases fail. Former employers often mistake the "duty of loyalty" that they believe their employees owe (including even former employees) for trade secret misappropriation. Thus, in many ways, trade secret cases are the personal injury cases of business litigation because the asserted loss of (and threats to) business assets often lead courts to react positively to the plaintiff's claims before there is clear proof of the existence of a trade secret. Particularly at the preliminary relief stage, courts often minimize plaintiff's burden of proving the existence of trade secrets when there is evidence of bad acts, such as surreptitious copying of materials on a copying machine or downloading information to a jump drive. In effect, judges are blinded by

the asserted wrongs. This is where the potential for abuse arises and why a powerful new form of preliminary relief is troublesome.

Because of the foregoing, the opponents of the DTSA are very concerned about how the DTSA may affect employee mobility. The proponents argue that the language which reads "provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation described in paragraph (1)" is sufficient to protect employees. However, this language only addresses potential remedies by directing the courts to consider the impact of any injunction on employment. It does not address the broader concern about how expanded trade secret rights and remedies might be used to intimidate and control employees before litigation is even filed or, if it is filed, before a decision on the merits of the case. It also does not reject the inevitable disclosure doctrine or allow existing state law to apply with respect to such issue.

The proponents of the DTSA who appeared at the recent hearing characterized the controversial "inevitable disclosure doctrine" as merely circumstantial evidence of "threatened misappropriation." However, the inevitable disclosure argument is typically raised in trade secret cases when there is little or no evidence that any tangible embodiments of trade secrets have been taken or maintained by the former-employee/defendant or when there is little evidence of threatened disclosure or use of the alleged trade secrets. The focus of the argument is on information that the former-employee/defendant has stored in her brain. The problem is that there is a fine-line between legitimate trade secrets stored in an individual's brain and the general skill and knowledge that individuals gain on the job.[27]

Unfortunately, for a variety of reasons (including the emotional reasons just mentioned), the reasonable efforts requirement of trade secrecy is not always applied stringently enough to preclude former-employees from being subjected to claims of trade secret misappropriation under circumstances where they had little or no prior notice of what their former employer claimed as a trade secret.[28] Also, the true extent of threats of trade secret litigation that are made against former employees is unknown because such threats typically take the form of a cease and desist letter first, only resulting in trade secret litigation if the former employee does not accept the former employer's demands. Often, employees who are served with cease and desist letters do not have the financial means to hire an attorney to advise them concerning the validity of such claims and, thus, readily agree to their former employer's demands. To the extent such demands overreach and require employees not to accept particular employment, they restrict employee mobility and are anticompetitive.

---

[27] *See* James H A. Pooley, *Restrictive Employee Covenants in California*, 3 Santa Clara High Tech. L.J. 251, 281 (1988) (explaining that "it is exceedingly difficult to draw a line between an employer's enforceable proprietary rights and the employee's general knowledge and skills").

[28] *See* David S. Levine, *School Boy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation*, 72 Wash. & Lee L. Rev. Online 323 (2015) (expressing concern that the DTSA will lead to even less stringent examination of the reasonable efforts requirement).

Unless putative trade secret owners engage in sufficient reasonable efforts to protect their trade secrets, particularly with respect to identifying claimed trade secrets, employees may actually be unaware of what information should be treated as a trade secret. Thus, while I remain opposed to the inevitable disclosure doctrine for the reasons expressed by California courts,[29] if and where the inevitable disclosure doctrine is applied, putative trade secret owners should be held to a heightened burden of proving that the subject employee was actually informed by her employer of the precise information that should be treated as a trade secret. This is particularly important with low-level and low-paid employees who do not regularly (or ever) deal with the proprietary information of their employers.

To avoid the misuse of the seizure remedy against former employees, an exemption is a possible answer. The key is to differentiate between the types of cases that are used to justify the seizure remedy (largely, espionage and wrongful acquisition cases) from the more typical trade secret case involving former employees and an alleged breach of a duty of confidence). This might be accomplished in several ways.

First, as I mentioned in my testimony, the DTSA should be amended to make it clear that it is to be interpreted in accordance with the commentary to the UTSA, which includes reference to many more limitations on the scope of trade secret rights than are contained in the DTSA. It should also be made clear that trade secrets do not include the general skill and knowledge that employees learn on the job.

Second, as Senator Whitehouse suggested, employee cases might be exempted altogether from the seizure remedy. At a minimum, I suggest that cases against former employees require evidence of an express confidentiality agreement and advance and direct notice to the subject employee that the information that is the subject of litigation was claimed as the employer's trade secret. Employees should not be sued for trade secret misappropriation and subjected to a seizure order (or criminal prosecution) when they had no prior knowledge of what their employer claimed as a trade secret. Unfortunately, the DTSA (and UTSA) scienter requirement of "knowledge or reason to know" is often applied too liberally in emotionally charged trade secret cases.

Third, the DTSA might be amended to include a provision similar to one that is contained in the proposed EU Trade Secret Directive. Article 13.1a of the draft Directive provides: "In accordance with their national law and practice, Member States may limit the liability for damages of employees towards their employers for the unlawful acquisition, use or disclosure of a trade secret of the employer when they act without intent."

[29] Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443 (2002).

In conclusion, I am concerned that the problem of trade secret misappropriation is being viewed primarily through the lens of large trade secret owners and not defendants (usually former employees and start-up companies) who are wrongly accused of trade secret misappropriation. If these individuals and companies survive an early trade secret misappropriation action brought against them, perhaps they are around to speak up about the pitfalls of an unbalanced system, but if they are not (and my experience tells me many are not), someone has to point out that there are two sides to the trade secret misappropriation story. The existing system of state laws, which is largely uniform, does a good job of balancing the interests of legitimate trade secret owners with those that are accused of trade secret misappropriation. Particularly because there is no existing federal jurisprudence with respect to civil trade secret claims and the DTSA does not include many of the limitations on the scope of trade secret protection that exist under state trade secret law, I am afraid the DTSA lacks the balance that is needed to prevent it from being abused.

Thank you for the opportunity to submit this letter and to testify concerning these important issues. If I can provide any additional information or insights, I am happy to do so.

Sincerely,

Sharon K. Sandeen

Sharon K. Sandeen
Professor of Law
Mitchell | Hamline School of Law
sharon.sandeen@mitchellhamline.edu