

1-7-2016

DTSA: A Federal Tort of Unfair Competition in Aerial Reconnaissance, Broken Deals, and Employment

Stephen Y. Chow
Burns & Levinson LLP

Follow this and additional works at: <https://scholarlycommons.law.wlu.edu/wlulr-online>



Part of the [Intellectual Property Law Commons](#)

Recommended Citation

Stephen Y. Chow, *DTSA: A Federal Tort of Unfair Competition in Aerial Reconnaissance, Broken Deals, and Employment*, 72 WASH. & LEE L. REV. ONLINE 341 (2015), <https://scholarlycommons.law.wlu.edu/wlulr-online/vol72/iss2/7>

This Roundtable: The Defend Trade Secrets Act of 2015 is brought to you for free and open access by the Law School Journals at Washington & Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review Online by an authorized editor of Washington & Lee University School of Law Scholarly Commons. For more information, please contact lawref@wlu.edu.

DTSA: A Federal Tort of Unfair Competition in Aerial Reconnaissance, Broken Deals, and Employment

Stephen Y.
Chow*

Abstract

This Essay critiques the creation by the 114th Congress of a federal private right of action under the Defend Trade Secrets Act for the state unfair competition cause of trade secret misappropriation hitherto applied mostly to breaches of express or implied confidential relationships between businesses or with employees. The proposed insertion of the Uniform Trade Secrets Act definition of “misappropriation,” including acquisition by “improper means” exemplified by state commercial mores’ expectation of privacy from aerial reconnaissance, into the Economic Espionage Act framework of theft of a more narrowly defined “trade secret” of a defined “owner,” including such actions abroad by American companies, opens litigation opportunities that are unlikely to fulfill the purposes of the legislation. There is no current need to “harmonize” compliance programs, and the non-preemptive legislation would simply add more issues to be litigated in multiple contexts, including disputes over privacy or confidentiality managed by online terms. The legislation’s limitation of injunctions under a promise of “employee mobility” threatens state practices of contractual restrictions on post-employment competition.

* Partner, Burns & Levinson LLP, Boston, Massachusetts; Adjunct Professor Suffolk University Law School, Boston, Massachusetts; Uniform Law Commissioner, Massachusetts.

Table of Contents

I. Introduction.....	342
II. UTSA “Misappropriation” Is Unfair Competition in Use of Open-Ended “Trade Secrets”	345
III. EEA Is Directed to “Theft” or “Conversion” of Narrower, “Owned” Manifestations	350
IV. There Is No Present Need to Have Multiple Trade Secret Compliance Plans	353
V. DTSA Is “Not Ready for Prime Time”	355
A. A Federal Cause of Action for Unfair Competition Should Be Better Studied	355
B. Does DTSA’s Promise of “Employee Mobility” Preempt Non-Compete Agreements?	357
VI. Conclusion	358

I. Introduction

The Defend Trade Secrets Act of 2015 (“DTSA”)¹ would create a federal private right of action under the Economic Espionage Act (“EEA”)² for the state unfair competition tort of “misappropriation,” which is defined under the Uniform Trade Secrets Act (“UTSA”) to include acquisition of competitively valuable information by “improper means” or use in breach of a contractual or other duty “to maintain its secrecy or limit its use.”³

1. Defend Trade Secrets Act of 2015, H.R. 3326 & S. 1890, 114th Cong. (2015).

2. 18 U.S.C. §§ 1831–1839 (2012).

3. The UTSA was promulgated in 1979 and revised in 1985 by the National Conference of Commissioners on Uniform State Laws. Unif. Trade Secrets Act (1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf. It has been adopted in forty-seven states, *Legislative Fact Sheet—Trade Secrets Act*, UNIF. L. COMM’N (2015), <http://www.uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act> (last visited Oct. 25, 2015) [hereinafter UTSA] (on file with the Washington and Lee Law Review), and adopted in substance in North Carolina, N.C. GEN. STAT. §§ 66-152–66-157 (2015).

Over the nearly two centuries of using this branch of state unfair competition law,⁴ the overwhelming portion of cases have involved unauthorized use of information lawfully acquired in broken business deals and by employees who leave and compete.⁵ The only paradigm for non-fraudulent, non-trespassory “improper means” remains aerial reconnaissance as against “commercial morality.”⁶ The current proliferation of aerial drones with cameras may see challenges through UTSA or DTSA actions, if not by self-help.

The DTSA’s sponsors justify their departure from tort reform with the need to combat alleged theft of American trade secrets, valued at twelve figures annually, including theft through foreign cyber-espionage and theft of the embodiments of trade secrets such as trespass to steal experimental seeds.⁷ This Essay questions whether the DTSA’s contribution to solving these problems⁸ is outweighed by clear societal costs⁹—including those

4. See *Vickery v. Welch*, 36 Mass. 523, 525 (1837) (regarding a restrictive covenant on the secret art of making chocolate); RESTATEMENT (FIRST) OF TORTS §§ 757–759 (AM. LAW INST. 1939) (addressing trade secrets); RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39–45 (AM. LAW INST. 1995) (addressing trade secrets).

5. See David S. Almeling, et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 60–61 (2010) (“[T]he alleged misappropriator was an employee or a business partner 93% of the time in this state study. That figure was comparable to that of the federal study, which showed the alleged misappropriator to be an employee or a business partner in 90% of cases.”).

6. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475–76 (1974) (citing *E. I. du Pont de Nemours & Co. v. Christopher*, 431 F.2d 1012 (5th Cir. 1970)). Aerial reconnaissance is also discussed as an example of possibly improper means in the UTSA. UTSA, *supra* note 3, § 1 cmt.

7. See 161 CONG. REC. S7250–51 (daily ed. Oct. 8, 2015) (statement of Sen. Hatch) (discussing the impact of trade secret theft).

8. Cyber-theft typically is perpetrated by depositing malware through “spearphishing”—tricking insiders to open malware files through believable emails (such as apparently from a trusted person). Other than apprehending the sender (which DTSA does not provide for, but existing EEA does) the solutions include insider discipline as to secure practices, malware detection, and restriction of internal access, which are not subjects of DTSA. Other foreign agent theft is already addressed by existing EEA and fits within diversity federal diversity jurisdiction. “Stings” or “entrapment” of suspect insiders are available under existing EEA, but not under UTSA or DTSA.

9. Proponents have identified a swing from patent disclosure to trade secret non-disclosure (as was prevalent in the 1970s, see UTSA, *supra* note 3, at Prefatory Note), because of the elimination of the “best mode” requirement for

of American businesses—in establishment of a not-quite-parallel-to-UTSA federal tort of unfair competition applied in practice mostly to broken deals and exiting employees.

The DTSA may backfire by enabling—through its minimal jurisdictional requirements¹⁰—and incentivizing¹¹ suits by non-practicing entities¹² and foreign entities for breaches of foreign duties.¹³ Even if it does not, by failing to preempt state trade

patents, the limitation of the effect of “secret use” on patentability, and the expansion of prior use rights by the Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011). Such “siloining” of knowledge arguably led to the downfall of the mini-computer giants of 1980s Massachusetts.

10. DTSA § 2 creates a new 18 U.S.C. § 1836(b)(1) cause for an “owner of a trade secret,” defined at existing §§ 1839(3)–(4), “who is aggrieved by a [UTSA] *misappropriation* of a trade secret that is *related to a product or service* used in, or *intended for use* in, interstate or foreign commerce.” Defend Trade Secrets Act of 2015, H.R. 3326 & S. 1890, 114th Cong. § 2(a) (2015) (emphasis added). This is considerably broader than the “theft of trade secrets” offense of EEA that requires an “intent to *convert . . . to the economic benefit of anyone other than the owner* thereof, and intending or *knowing that the offense will injure any owner* of that trade secret” and knowing theft, transmission, receipt, attempt, or conspiracy. 18 U.S.C. § 1832 (2012) (emphasis added). There is no jurisdictional amount required, as in diversity jurisdiction, or by many state courts of general jurisdiction. *See* H.R. 3326 & S. 1890 § 2 (addressing federal jurisdiction for theft of trade secrets).

11. Overlooking the UTSA § 3 Comment that the section authorizes double exemplary damages in addition to actual recovery, DTSA on its face authorizes triple exemplary damages. H.R. 3326 & S. 1890 § 2(a) (providing for triple damages under proposed 18 U.S.C. § 1836(b)(3)(C)). DTSA allows the trade secret plaintiff to wait five years to sue while the defendant develops a market and collects revenues—two more years than UTSA § 6. *See id.* § 2(d) (providing the period of limitations).

12. This is the broad definition of “troll” for a patent, ownership of which by itself does not merit, since *eBay Inc. v. MercExchange, LLC*, 547 U.S. 388 (2006), an injunction against further infringement unless there is irreparable injury threatened, for example, to the good will of an owner that practices the patented invention. Under the UTSA, injunction against use of a “secret” may be enjoined as irreparable “disclosure” (typically in violation of a non-disclosure agreement) even if the plaintiff does not use the “secret.” Some proponents of the DTSA dismiss application of the much narrower “troll” business model of “holding up” multiple defendants because UTSA misappropriation is an intentional tort unlike the strict liability infringement of patents, that is, trade secrets are not “property” like patents (even weakened by *eBay*).

13. Existing 18 U.S.C. § 1837 expressly allows application of “the chapter” to conduct occurring outside the United States if “the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof . . .” DTSA places in the chapter a private right of action for UTSA misappropriation—including acquisition by “improper means”

secret misappropriation law and setting up a not-quite-parallel federal regime, DTSA exposes significant issues to be litigated in both regimes. Such litigation not only increases the cost of protecting trade secrets, but may narrow the adopted EEA “trade secret” definition in ways not previously challenged by criminal defense lawyers who represented individuals with limited resources.

Litigation over these issues may affect the law of business and employment relationships involved in most trade secret cases, including concepts of express and implied consent, contracts, and expectations of privacy. Indeed, the DTSA sponsors expressly recorded in the legislative history its policy of “employee mobility,” that the DTSA “states explicitly that a person cannot be prevented from accepting an offer of employment because of his or her prior exposure to trade secrets.”¹⁴ As discussed below, if this language survives through enactment, there is much to argue as to its effects, if any, on employee non-compete agreements, a mainstay of non-Californian American business.

Many of these issues stem from the mismatch of the UTSA codification of the unfair competition of use of information in breach of a duty “to maintain its secrecy or limit its use” or acquired by “improper means” with the more narrowly targeted EEA criminal theft or conversion of a “trade secret.”

II. UTSA “Misappropriation” Is Unfair Competition in Use of Open-Ended “Trade Secrets”

A wide range of conduct has been called “misappropriation,” such as copying products or “free-riding” on another’s achievements in the market. Misappropriation is also called “unfair competition” by some aggrieved parties.

Congress has not granted a federal private right of action for general unfair competition as, for example, addressed under the

viewed against commercial morality and duties attached to relationships to maintain secrecy or limit use. See H.R. 3326 & S. 1890 § 2 (defining “misappropriation” and “improper means”).

14. 161 CONG. REC. S7252 (daily ed. Oct. 8, 2015) (statement of Sen. Hatch).

Federal Trade Commission Act.¹⁵ It has acted under the Commerce Clause to create (1) a federal private right of action under the Lanham Act for unfair competition in misappropriation of commercial identity—originally, and still primarily, of federally registered trademarks¹⁶; and (2) a federal private right of action under the Copyright Act for misappropriation of unpublished works previously protected under state law.¹⁷

Unfair competition through trade secret misappropriation involves many more legal issues than are raised by copying a trademark that the public has associated with a source or an unpublished manuscript. In the earliest American cases, “trade secrets” were defined as the knowledge of someone who acquired it lawfully in commerce, including employment, but who was bound by some “confidential” relationship to limit its use and disclosure.¹⁸ The wrong occurred in the breach of that duty of confidentiality. If the duty was created by contract, the wrong would be a breach of contract. If it was created by a recognized fiduciary, confidential, or agency relationship, the wrong would

15. 15 U.S.C. § 45 (2012). In contrast many states have “Baby FTC Acts” that *do* grant such private rights of action, often used against trade secret misappropriation. *E.g.*, MASS. GEN. LAWS ANN. ch. 93A, §§ 2 & 11 (West 2015).

16. 15 U.S.C. §§ 1114–1129 (2012). DTSA proponents cite the coexistence of the Lanham Act and state unfair competition (trademark) law to support the creation of a dual system of civil trade secret misappropriation law. The analogy is inapt because of the much greater interaction of the UTSA with different bodies of state law as outlined in this Essay and the particularly open-ended UTSA “trade secret.” The DTSA’s adaptation of the Lanham Act provision for specified time and space civil seizure of counterfeits of federally registered trademarks (and not merely unauthorized distribution), 15 U.S.C. §§ 1116(d), is hardly applicable to ideas in a person’s memory. *See* Defend Trade Secrets Act of 2015, H.R. 3326 & S. 1890, 114th Cong., § 2(a) (2015) (providing requirements of civil seizure).

17. 17 U.S.C. § 301(a) (2012) (preempting state law). The Commerce Clause, U.S. CONST. art. 1, § 8, cl. 3, was a back-up argument for the change from pre-1976 publish-with-notice-for-limited-monopoly as the *quid pro quo* under the Patent and Copyright Clause, U.S. CONST. art. 1, § 8, cl. 8. Some have suggested the AIA’s cut-back on disclosure also challenges that *quid pro quo*.

18. *See* Peabody v. Norfolk, 98 Mass. 452, 461–62 (Mass. 1868) (regarding confidential employment and “secrets of trade”); Vickery v. Welch, 36 Mass. 523, 525 (1837) (regarding trade secrets following the sale of a chocolate factory); Peter Andreas, *Piracy and Fraud Propelled the U.S. Industrial Revolution*, BLOOMBERGVIEW (Feb. 1, 2013), <http://www.bloomberglaw.com/articles/2013-02-01/piracy-and-fraud-propelled-the-u-s-industrial-revolution> (last visited Oct. 19, 2015) (on file with the Washington and Lee Law Review).

be a breach of that duty. What trade secret misappropriation law added was recognition of non-contractual, non-fiduciary duties arising in business negotiations and sales, which overlap fraud-type “improper means” of acquisition.¹⁹

In cataloguing its torts, the 1939 *Restatement* expressly rejected a “property” theory of entitlement: “The suggestion that one has a right to exclude others from the use of his trade secret because he has a right of property in the idea has been frequently advanced and rejected.”²⁰

State causes of action for “misappropriation” by copying publicly available product design were found to have been preempted by federal patent law in the 1964 case *Sears, Roebuck & Co. v. Stiffel Co.*²¹ In 1974, the Supreme Court in *Kewanee v. Bicron*²² cleared from such preemption the following types of trade secret “misappropriation”:

The protection accorded the trade secret holder is against the disclosure or unauthorized use of the trade secret by those to whom the secret has been confided under the express or implied restriction of nondisclosure or nonuse. The law also protects the holder of a trade secret against disclosure or use when the knowledge is gained, not by the owner’s volition, but by some “improper means,” Restatement of Torts § 757(a), which may include theft, wiretapping, or even aerial reconnaissance.²³

The 1939 *Restatement* described “improper means of discovery” as those that “fall below the generally accepted standards of commercial morality and reasonable conduct.”²⁴ The

19. See RESTATEMENT (FIRST) OF TORTS § 757 (AM. LAW INST. 1939) (addressing improper means and also acquisition by mistake). Section 758 restates rules for innocent acquisition. Section 759 restates a cause for procurement by “improper means” of business information not rising to the level of 1939 RESTATEMENT’s “trade secrets” as defined in comment b to section 757.

20. *Id.* § 757 cmt. a.

21. 376 U.S. 225, 230–31 (1964) (“[T]he patent system is one in which uniform federal standards are carefully used to promote invention while at the same time preserving free competition.”).

22. 416 U.S. 470 (1974).

23. *Id.* at 475–76.

24. RESTATEMENT (FIRST) OF TORTS § 757 cmt. f (AM. LAW INST. 1939) (including as examples acquisition by physical force, “fraudulent misrepresentations to induce disclosure, tapping of telephone wires, eavesdropping or other espionage”); see also *id.* § 759 cmt. c

Kewanee Court added the aerial reconnaissance example of *E.I. du Pont de Nemours & Co. v. Christopher*,²⁵ explaining: “The maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law. ‘The necessity of good faith and honest fair dealing, is the very life and spirit of the commercial world.’”²⁶ The *Christopher* court reasoned:

The Supreme Court of [Texas] has declared that “the undoubted tendency of the law has been to recognize and enforce higher standards of commercial morality in the business world.” . . . To obtain knowledge of a process without spending the time and money to discover it independently is improper unless the holder voluntarily discloses it or fails to take reasonable precautions to ensure its secrecy. . . . Perhaps ordinary fences and roofs must be built to shut out incursive eyes, but we need not require the discoverer of a trade secret to guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available.²⁷

State support of an expectation of respect of reasonable precautions against information-gathering without fraud or physical trespass may be considered recognition of commercial privacy.²⁸

The 1979 UTSA greatly expanded the 1939 *Restatement’s* definition of a “trade secret,” which was defined as “a process or

Among the means which are improper are theft, trespass, bribing or otherwise inducing employees or others to reveal the information in breach of duty, fraudulent misrepresentations, threats of harm by unlawful conduct, wire tapping, procuring one’s own employees or agents to become employees of the other for purposes of espionage

25. 431 F.2d 1012 (5th Cir. 1970).

26. *Kewanee Oil*, 416 U.S. at 481–82 (citation omitted).

27. *Christopher*, 431 F.2d at 1015–16.

28. Compare RESTATEMENT (FIRST) OF TORTS § 867 (AM. LAW INST. 1939) (“A person who unreasonably and seriously interferes with another’s interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other.”), and RESTATEMENT (SECOND) OF TORTS § 625B (AM. LAW INST. 1977) (“One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”), with RESTATEMENT OF EMPLOYMENT LAW § 7.03 (AM. LAW INST. 2015) (providing the employee’s expectation of privacy in physical and electronic spaces).

device for continuous use in the operation of the business.”²⁹ The UTSA provides that:

“Trade secret” means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.³⁰

“The broader definition . . . extends protection to a plaintiff who has not yet had an opportunity or acquired the means to put a trade secret to use.”³¹ The UTSA makes clear that it applies to *any* “information” that meets the stated qualifications.³²

As in the 1939 *Restatement*, the UTSA is not based on a property theory of entitlement: “The Uniform Act codifies the basic principles of common law trade secret protection, preserving its essential distinctions from patent law. Under both the Act and common law principles, for example, more than one person can be entitled to trade secret protection with respect to the same information”³³

Unlike a patent published with its claims (metes and bounds) and ownership registered with the U.S. Patent & Trademark Office, “trade secrets” are amorphous—dependent on situational

29. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939) (defining “trade secret”).

30. Unif. Trade Secrets Act § 1(4) (1985) (emphasis added).

31. *Id.* § 1 cmt.

32. Notably these do not include the fifth of the six factors listed in RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939) (“[T]he amount of effort or money expended by him in developing the information.”).

33. Unif. Trade Secrets Act, Prefatory Note (1985). *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986 (1984) found in a “taking” analysis a “property interest” in documents submitted to the government designated “trade secret.” “Fee simple” ownership, however, has been rejected as a Maryland UTSA requisite. *DTM Research, L.L.C. v. AT&T Corp.*, 245 F.3d 327, 332 (4th Cir. 2001) (“[C]onceptual difficulty arises from any assumption that knowledge can be owned as property.”). *Accord* *Advanced Fluid Systems, Inc. v. Huber*, 28 F. Supp. 3d 306, 318–23 (M.D. Pa. 2014) (providing the same for Pennsylvania’s UTSA).

value and effort to keep secret—particularly UTSA “trade secrets” that may be ideas held in the minds of several people. The UTSA does not define an “owner,” but creates a tort remedy for acquisition by “improper means” or unauthorized use in breach of a confidential relationship—where entitlement of the plaintiff is based on the liability of the tortfeasor.

The 1995 *Restatement of Unfair Competition* embraced the principles of the UTSA, noting that, “[m]any cases acknowledge that the primary issue is the propriety of the defendant’s conduct as a means of competition” and that

[t]he definition of a trade secret contained in this Section [consistent with the UTSA] . . . is directly applicable only to the imposition of civil liability under the rules stated in § 40. It does not apply, other than by analogy, in actions under criminal statutes or in other circumstances not involving civil liability for the appropriation of a trade secret³⁴

III. EEA Is Directed to “Theft” or “Conversion” of Narrower, “Owned” Manifestations

Contrary to the 1995 *Restatement’s* caution, the EEA criminal statute was enacted the following year by the 104th Congress as a combination of H.R. 3723 and S. 1556 with a definition of “trade secret” similar to that of UTSA § 1(4) but shown here to be much narrower:

H.R. 3723, the Economic Espionage Act of 1996, creates a new crime of wrongfully copying or otherwise controlling trade secrets, if done with the intent either to (1) benefit a foreign government, instrumentality, or agent, or (2) disadvantage the rightful owner of the trade secret and for the purpose of benefitting another person. . . .³⁵

S. 1556, addressed to “proprietary economic information,” specifically protected employees:

The bill explicitly states that the term proprietary economic information does not include the general knowledge, skills or

34. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (AM. LAW INST. 1995) (“The concept of a trade secret as defined in this Section is intended to be consistent with the definition of ‘trade secret’ in § 1(4) of the [UTSA].”).

35. H.R. REP. NO. 104-788, at 3 (1996) (emphasis added).

experience that a person has. A prosecution under this statute must establish a particular piece of information that a person has stolen or misappropriated. It is not enough to say that a person has accumulated experience and knowledge during the course of his or her employ. Nor can a person be prosecuted on the basis of an assertion that he or she was exposed to proprietary economic information while employed. . . .

. . . .

“Proprietary economic information” is defined as a type of intellectual property connoted by four characteristics: (1) it is proprietary; (2) its nature is economic, business, scientific, technical, or engineering; (3) it consists of information, data, plans, tools, mechanisms, compounds, formulas, designs, prototypes, processes, procedures, programs, codes, or commercial strategies; and (4) it derives value from its exclusivity. These features distinguish it from other forms of intellectual property, such as literary or artistic works. [It] also does not include general knowledge, experience, training, or skill acquired by a person as a result of his or her employment or hire by any owner.³⁶

The EEA adopted a definition of “trade secrets” that did not include the definition of “commercial strategies” that was included in the otherwise similar S. 1556 and definition of “proprietary economic information”:³⁷

(3) the term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not

36. S. REP. NO. 104-359, at 12–14 (1996).

37. Compare 18 U.S.C. § 1839(3) (2012), with H.R. REP. NO. 104-788, at 2, and S. REP. NO. 104-359, at 2.

being readily ascertainable through proper means by, the public³⁸

Despite explanations in the reports that the EEA “trade secret” definition is based on the UTSA,³⁹ the language is substantively different. In a case of “more is less,” the longer list of examples and characterizations, combined with the narrow reading to be given terms in a criminal statute, as well as usage within EEA to support its objective of punishing “theft” and “conversion,” particularly with the additional express (if vague) definition of ownership, EEA “trade secrets” are very arguably a subclass of UTSA “trade secrets” that do not include mentally held “knowledge, skills and experience.”

The UTSA uses open-ended “including” examples for unrestricted “information”; EEA uses “including” examples for express categories of information, omitting categories such as “cultural,” “literary,” and “strategic.” The language quoted from the Senate Report ruled out “literary or artistic” categories.

The EEA characterizes its examples as being “stored, compiled, or memorialized”—not learned, known, or remembered—“physically, electronically, graphically, photographically, or in writing”—not mentally as the ideas protected by the UTSA as recognized in the 1995 *Restatement*.⁴⁰

The base EEA §§ 1831 and 1832 offenses of “theft” and “conversion” apply most clearly to physical objects or records, including “electronic” (which was considered during the 1990s to be “intangible”)—rather than mental knowledge. “Conversion” (intent required by both sections) is wrongful control over chattels, including documents into which “intangible rights are merged,” such as motion picture film.⁴¹ In accordance with the purpose of the EEA quoted above, the government is “required to

38. § 1839(3).

39. S. REP. NO. 104-359, at 14; H.R. REP. NO. 104-788, at 12.

40. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (AM. LAW INST. 1995). *See also id.* cmt. d (“The appropriation of an idea offered to another through an oral presentation . . . can be actionable under the law of trade secrets.”).

41. RESTATEMENT (SECOND) OF TORTS §§ 222A(1) & 242 cmt. b (AM. LAW INST. 1965).

prove that the defendant has wrongfully copied or otherwise exerted control over [that is, converted] a ‘trade secret.’”⁴²

EEA § 1832 theft expressly refers to the “owner,” and the EEA defines owner as “the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.”⁴³ The UTSA does not define ownership. EEA’s reference to “rightful legal or equitable title” has unclear application to trade secrets that, unlike real property, patents, copyrights or statutory trademarks, are registered and provide notice of their scope.⁴⁴ The alternative of “license” is even less clear, as licenses are presumed to be non-exclusive. Even exclusive licensees may not have standing to sue under other intellectual property law. The EEA concept of ownership fits with its concern over theft and conversion of physical (including electronic) manifestations of trade secrets and not with “knowledge, skills and experiences,” at least the “general” ones excluded by the Senate Report.⁴⁵

If disputed, the EEA definition of “trade secret” will be strictly construed as a part of a criminal statute.⁴⁶ Deep-pocketed parties may argue one or more of the above in a DTSA suit—and by winning may also limit future prosecution under the criminal provisions of the EEA.

IV. There Is No Present Need to Have Multiple Trade Secret Compliance Plans

42. H.R. REP. NO. 104-788, at 7 (1996).

43. 18 U.S.C. § 1839(4) (2012).

44. See RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939) (including notice as a factor).

45. S. REP. NO. 104-359, at 12–13 (1996). The elimination of the “commercial strategies” example is consistent with the exclusion of mental knowledge, rather than documents and other chattel manifesting secrets. See *supra* note 37 and accompanying text (noting the EEA’s exclusion of “commercial strategies”).

46. *United States v. Aleynikov*, 676 F.3d 71, 75–76 (2d Cir. 2012) (construing the original EEA jurisdictional “produced for . . . interstate or foreign commerce” definition strictly (citing *Dowling v. United States*, 473 U.S. 207, 213 (1985))); cf. *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012) (applying the Computer Fraud and Abuse Act “rule of lenity” in civil action).

Notwithstanding the arguably narrower applicability of EEA “trade secrets,” it simply is not true, as DTSA proponents stated for the 2014 predecessor bill, that the state enactments of the UTSA “require companies to tailor costly compliance plans to meet each individual state’s law.”⁴⁷ Under the EEA, the UTSA, and the 1939 *Restatement*, only one compliance plan is required: one must do what is “reasonable” to keep the information sought to be protected “secret.”⁴⁸

The relatively few enforcement differences between particular UTSA enactments do not affect what can and should be done to protect information intended to be protected by the USTA or EEA definitions of “misappropriation” or “theft.” Variations by six states and the EEA of the UTSA § 1(4)(i) qualification of “not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use”⁴⁹ also do not

47. H.R. REP. NO. 113-657, at 7 (2014). Nor is enactment of the DTSA necessary to establish a “single national baseline” of “minimum protection,” as now suggested by the sponsors for its harmonization without preemption. *See* 161 CONG. REC. S7251 (daily ed. Oct. 8, 2015) (statement of Sen. Coons). It already exists.

48. The EEA requires “reasonable measures to keep such information secret.” 18 U.S.C. § 1839(3)(A) (2012). UTSA § 1(4)(ii) requires “efforts that are reasonable under the circumstances to maintain [the protected information’s] secrecy.” Among the UTSA states, only Colorado requires “measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes,” COLO. REV. STAT. § 7-74-102(4) (2015), but the same baseline of “reasonable efforts” or “reasonable measures” would appear to meet this requirement. A New York intermediate appellate court (one of the two non-UTSA states) has cited the 1995 *Restatement* that adopted the UTSA definition with approval. *E.g.* *Wiener v. Lazard Freres & Co.*, 241 A.D.2d 114, 124, 672 N.Y.S.2d 8, 15 (N.Y. App. Div. 1998). The other non-UTSA state, Massachusetts, has adopted the 1939 *Restatement*. *See* *J.T. Healy & Son v. James A. Murphy & Son*, 260 N.E.2d 723, 738 (1970) (“But if the person entitled to a trade secret wishes to have its exclusive use in his own business, he must not fail to take all proper and reasonable steps to keep it secret.”). The 1939 *Restatement* includes a requirement of “a substantial element of secrecy,” measured by factors including “the extent of measures taken by him to guard the secrecy of the information.” RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939).

49. *See* CAL. CIV. CODE § 3426.1(d)(1) (Deering 2015) (“[N]ot being generally known to the public or to other persons who can obtain economic value from its disclosure or use.”); 765 ILL. COMP. STAT. 1065/2(d)(1) (2015) (“[N]ot being generally known to other persons who can obtain economic value from its disclosure or use.”); NEB. REV. STAT. § 87-502 (2015) (“[N]ot being known to, and

affect what can and should be done to protect secrets. Whether a purported secret is “generally known to” or “readily ascertainable by” an undefined “public” as in the EEA or a relevant public as specified by the UTSA, that knowledge is outside the control of a compliance plan.

Issues arise not from the different emphases of UTSA variants, but from non-disclosure agreements that cast a wide net without providing meaningful notice, unaccompanied by other efforts to ensure security of valuable information. Often obligations sunset for the convenience of business associates.

Instead of preventing unfair competition by targeting unauthorized use of specific information, employers use the less expensive, blunt instrument of prohibiting post-employment competition altogether for a time that is related less to the “shelf life” of the information than to the ability of most employees to forego employment doing what they have gained experience doing.

V. DTSA Is “Not Ready for Prime Time”

A. Any Federal Cause of Action for Unfair Competition Should Be Better Studied Before Implementation

Congress has been circumspect about creating federal private rights of action for unfair competition and should remain so. A federal cause of action for unfair competition based on terms such as the DTSA’s “improper means,” “consent,” and “duty to maintain secrecy or to limit use,” if it succeeds in opening federal courts to a significant number who cannot avail now (assuming these exist), will result in more frequent and perhaps more

not being ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.”); N.C. GEN. STAT. § 66-152(3)(a) (2015) (“[N]ot being generally known or readily ascertainable through independent development or reverse engineering by persons who can obtain economic value from its disclosure or use.”); OR. REV. STAT. § 646.461(4)(a) (2015) (“[N]ot being generally known to the public or to other persons who can obtain economic value from its disclosure or use.”); S.C. CODE ANN. § 39-8-20(5)(a)(i) (2014) (“[N]ot being generally known to, and not being readily ascertainable by proper means by the public or any other person who can obtain economic value from its disclosure or use.”).

rigorous federal litigation of these terms, rather than state court litigation.

If it does not preempt the same UTSA terms, this likely would lead to greater disharmony, rather than the promised harmony. Even if not expressly preemptive, federal courts are likely to establish new constructions of UTSA or DTSA terms and may de facto preempt the more conservative operation of the “laboratories of democracy”—particularly because there is no DTSA counterpart to the UTSA § 8 deference to uniform development by the states.

With the rapid expansion of uses for inexpensive aerial drones, including surveillance, one expects that the *Christopher* precedent for aerial reconnaissance as “improper means” will be applied early—and perhaps often. Compared to a UTSA action, federal DTSA action may better withstand a preemption challenge under federal regulations that might be put in place, for example, by the Federal Aviation Administration.⁵⁰

Concurrent or separate decisions on DTSA “improper means,” “consent,” and “duty to maintain secrecy or to limit use” may affect the previous thirty years of federal court development of the terms “access . . . without authorization,” “exceed[ing] authorized access,” “agent,” and “lawful consent” in the federal anti-hacking Computer Fraud and Abuse Act (“CFAA”),⁵¹ the “wiretap” title of the Electronic Communication Privacy Act (“ECPA”),⁵² and the Stored Communications Act (“SCA”).⁵³ Common issues relating to expectations, authorized or proper

50. See Press Release, Fed. Aviation Admin., FAA Announces Small UAS Registration Rule (Dec. 14, 2015), http://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856 (last visited Dec. 16, 2015) (announcing a web-based aircraft registration process for owners of small unmanned aircraft) (on file with the Washington and Lee Law Review).

51. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2012). The Administration is currently proposing some modifications. See UPDATED ADMINISTRATION PROPOSAL: LAW ENFORCEMENT PROVISIONS, WHITE HOUSE (Jan. 13, 2015), <https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf> (last visited Dec. 16, 2015) (on file with the Washington and Lee Law Review).

52. Electronic Communication Privacy Act of 1986, 18 U.S.C. §§ 2510–2521 (2012).

53. Stored Communications Act of 1986, 18 U.S.C. §§ 2701–2709 (2012).

access by employees to the computer systems of their employers,⁵⁴ or visitors to “public” websites with restrictive online terms⁵⁵ span the small separation between personal privacy and the commercial privacy protected by the DTSA.

A difference from the current coexistence of UTSA, CFAA, ECPA, SCA, and other state law is that while the DTSA retains the EEA non-preemption of law, including state law, “for the misappropriation of a trade secret,”⁵⁶ there is nothing said about preemption of other law. Thus there is a question of whether the DTSA would preempt a breach of contract,⁵⁷ breach of confidentiality action, or the application of a contract to establish a duty of confidentiality.

B. Does DTSA’s Promise of “Employee Mobility” Preempt Non-Compete Agreements?

DTSA expressly restricts injunctions at proposed 18 U.S.C. § 1836(b)(3)(i): “provided the order does not prevent a person from accepting an offer of employment under conditions that avoid actual or threatened misappropriation.”⁵⁸ The sponsors put on the legislative record that the DTSA would not “restrict employee mobility” and “states explicitly that a person cannot be prevented from accepting an offer of employment because of his or her prior exposure to trade secrets.”⁵⁹

54. *E.g.*, *United States v. Nosal*, 676 F.3d 854, 856 (9th Cir. 2012) (en banc) (determining that authorization was not lost by non-work use of employer computer system).

55. *E.g.*, *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321–22 (11th Cir. 2006) (“Nothing inherent in any of these steps prompts us to infer that access by the general public was restricted.”).

56. *Defend Trade Secrets Act of 2015*, H.R. 3326 & S. 1890, 114th Cong. § 2(f) (2015); 18 U.S.C. § 1838 (2012).

57. *Cf.* *Uniform Trade Secrets Act*, § 7(b)(1) (1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf (last visited Oct. 20, 2015) (providing no effect on “contractual remedies, whether or not based upon misappropriation of a trade secret”) (on file with the Washington and Lee Law Review).

58. H.R. 3326 & S. 1890 § 2(a).

59. 161 CONG. REC. S7252 (daily ed. Oct. 8, 2015) (statement of Sen. Hatch). This appears to be a reversal of the declared neutrality of the 2014 predecessor bill on the “inevitable disclosure doctrine.” H.R. REP. NO. 113-657, at 12 n.9 (2014).

Does this express federal policy preempt an employee non-compete agreement premised on an employee's "prior exposure to trade secrets," as many such agreements need to be in order to be enforceable?⁶⁰ Reading the employee mobility proviso literally, would it allow an injunction to be written to bar the use of specific secrets? If so, may an employee subject to such a non-compete agreement justified by potential misappropriation of trade secrets (or their new employers) file declaratory judgment action to void or rewrite the agreement?

As the use of employee non-compete agreements is widespread, one would expect the employee mobility proviso to be removed or rewritten.

VI. Conclusion

The DTSA's federalization of UTSA "misappropriation" likely will not alter the current mix of trade secret cases founded in broken business deals and exiting employees, but may incentivize through the encouragement of private litigation new claims based on shared ideas, aerial surveillance, or web monitoring in "violation" of terms of service. The EEA definition of "trade secrets" adopted by the DTSA is arguably substantially narrower than that of the UTSA and may be further established as such through civil litigation by defendants with more resources than most EEA criminal defendants. Most importantly, while there has been no demonstration that differences in UTSA enactment or enforcement require different compliance programs that may

60. Generally under the common law, most states will enforce a restrictive covenant if it can demonstrate that the employer, "by means of a reasonably tailored restrictive covenant," protects the employer's "trade secrets . . . and other protectable confidential information." RESTATEMENT OF EMPLOYMENT LAW § 8.07(a)–(b)(1) (AM. LAW INST. 2015). The definition of "trade secrets" is similar to that of UTSA § 1(3), with a requirement of "reasonable measures." *Id.* § 8.02(b). "Confidential information" that is not "technically" a "trade secret" is protectable where the employee "was put on notice of which information the employer considered confidential and proprietary," but does not include information that would be considered part of the general experience, knowledge, training, and skills that an employee acquires in the course of employment." *Id.* § 8.07 cmt. b. A majority of states will rewrite ("blue pencil") the contract. *Id.* § 8.08, Reporters' Notes for cmt. a. But clearly there is difference among the states, notably California, which voids restraints on employment. CAL. BUS. & PROF. CODE § 16600 (Deering 2015).

be resolved by DTSA harmonization, the DTSA does not in fact harmonize. Instead, the DTSA creates dual private unfair competition litigation regimes with different definitions of “trade secrets” and limited preemption that likely will affect the scope of EEA “trade secrets,” employment law, and possibly online privacy. Thus, it would be prudent for Congress to act conservatively and rethink the DTSA.