NOTE

A FEDERALIST ACCOUNT OF THE LAW OF TRADE SECRECY

Martin J. Salvucci*

In May 2016, President Barack Obama signed the Defend Trade Secrets Act of 2016 (DTSA) into law.[1] Prior to the passage of the DTSA, trade secrets—unlike patents, copyrights, and trademarks—were protected largely by a patchwork of state laws.[2] Observers have described the passage of the DTSA—which, for the first time, creates a private cause of action under federal law for the misappropriation of trade secrets—as the most significant development for intellectual property law since the passage of the Lanham Act, which effectively federalized the law of trademarks in 1946.[3]

Even by the standards of intellectual property, trade secrets are especially vulnerable to theft. They are easily accessible and generally portable—and often, they are carried away in the mind's eye.[4] Their misappropriation is estimated to cost American firms as much as three percent of Gross Domestic Product—a figure that easily exceeds $300 billion.[5] And former FBI Director Louis Freeh once testified that stolen intellectual property resulted in the loss of

---

* A.B. 2010, University of Chicago; A.M. 2011, University of Chicago; J.D. 2018 (exp.), Stanford Law School. I am indebted to Kathryn Bi for bringing this topic to my attention, and for patiently answering a long series of elementary questions along the way. I am likewise grateful to Judge Thomas Ambro and David Freeman Engstrom for their critical feedback on prior drafts. As ever, the Mechanic's Lien Steering Committee offered a deep reservoir of encouragement, guidance, and support from which I drank regularly. And I am lastly quite thankful for the careful stewardship of Boyd Jackson, Elyssa Pak, Ashwin Aravind, and the rest of the editorial staff of the *Stanford Law & Policy Review*. All opinions expressed and any errors remain my own.

1. *See* Defend Trade Secrets Act of 2016, S. 1890, https://www.congress.gov/bill/114th-congress/senate-bill/1890/text.

2. *See* Christopher Seaman, *The Case against Federalizing Trade Secrecy*, 101 VA. L. REV. 317, 320-21 (2015).

3. *See id.* at 321.

4. JAMES POOLEY, TRADE SECRETS § 13.01 (1997).

5. *See generally* THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY, THE IP COMMISSION REPORT (2013), http://www.ipcommission.org/report/IP_Commission_ Report_052213.pdf.

more than one million American jobs—a substantial percentage of which, presumably, were attributable to the misappropriation of trade secrets.[6]

The DTSA amends an already-existing federal criminal statute—the Economic Espionage Act of 1996 (EEA)—to incorporate a private cause of action for misappropriation.[7] At the same time, the DTSA also expressly provides that already-existing state laws will not be preempted.[8] This decision is significant for two reasons. As a practical matter, it permits owners to retain the protections of the patchwork of state laws that previously served as their sole line of defense. In functional terms, moreover, this dynamic likely creates a novel federal-state system of protection, as well as an untested arrangement that will implicate significant doctrinal questions that pertain to federalism.

This paper asks what the DTSA can tell us about federal and state relations, what we call "Our Federalism" and *vice versa*. It proceeds in four parts. The first traces the history and the evolution of the law of trade secrecy from its beginnings in the nineteenth century through the development and widespread adoption of the Uniform Trade Secrets Act (UTSA). It also explores the subsequent passage of the EEA, as well as the debates that preceded the enactment of the DTSA. The second part examines the DTSA's jurisdictional element, which ostensibly limits what claims may proceed under federal law. It determines the available evidence—including both principles of statutory construction and albeit limited case law—does not answer how narrowly or broadly the jurisdictional element should be construed.

The third part takes up two values of Our Federalism—uniformity and experimentation—to argue for a narrow reading of the DTSA's jurisdictional element. Although it acknowledges that the DTSA likely will create what amounts to a "floor" for trade-secret protections, the third part argues that the anti-preemption provision will undercut the uniformity in protection and enforcement sought by the statute's proponents. Moreover, the third part takes up the example of so-called "inevitable disclosure" to contend that additional space for innovation at the state level is warranted. The fourth part offers some brief observations on likely trends in the law of trade secrecy.

PART ONE: THE PATH OF THE LAW

Scholars treat the law of trade secrecy as the "youngest sibling" among intellectual property's four major disciplines.[9] Unlike protections for patents and copyrights—whose longstanding statutory predicates ensured prominent

6. Adam Cohen, *Securing Trade Secrets in the Information Age: Upgrading the Economic Espionage Act after* United States v. Aleynikov, 30 YALE J. ON REG. 189, 192 n.20 (2013).

7. Defend Trade Secrets Act, *supra* note 1.

8. *See* 18 U.S.C. § 1838 (2016).

9. *See* Seaman, *supra* note 2, 323.

placement within the American Constitution[10]—the law of trade secrecy, much like the law of trademarks, emerged from a handful of common-law torts during the nineteenth century.[11] The emergence of trade secrets, in particular, followed the Industrial Revolution, which undermined well-established contractual norms.

A. *Trade Secrecy at Common Law*

Prior to the Industrial Revolution, "[t]he proprietary knowledge needed to practice a trade or craft often was passed from a master to an apprentice. In turn, the apprentice was contractually required to keep secret the know-how learned from the master."[12] But this contractual "restriction lasted only for the duration of the apprenticeship; afterward, the apprentice could 'freely depart with whatever skill and knowledge [he] had acquired.'"[13] Mass industrialization rendered those contractual arrangements largely impracticable due to a newly-mobile workforce, on the one hand, and a host of now readily observable industrial technologies on the other.[14]

The first reported protection for trade secrecy in the United States appears in 1837. In *Vickery v. Welch*, the Supreme Judicial Court of Massachusetts ordered specific performance of an agreement mandating the "exclusive" use of a secret method for cooking chocolate.[15] Subsequent decisions across jurisdictions continued to refine the scope of these protections: "The holder of a trade secret was required to take precautions to preserve its secrecy, but this secrecy did not have to be absolute. Information generally known to the public could not qualify as a trade secret. And an obligation not to disclose or use proprietary information was enforceable through an injunction."[16]

By the 1930s, the law of trade secrecy had attracted sufficient attention as to merit inclusion in the American Law Institute's *Restatement (First) of Torts* (*Restatement)*, which sought to bring a modicum of consistency and uniformity to the thicket of state tort-law regimes.[17] The *Restatement* defines a trade secret in relatively broad terms—as "any formula, pattern, device or compilation of information which is used in one's business, and which gives [its owner] an

---

10. U.S. CONST. art. I, § 8, cl. 8.

11. Statutory protections for patents date at least to the Venetian Statute of 1474 and the Statute of Monopolies in 1623. Statutory protections for copyrights, although less numerous, date at least to the Statute of Anne in 1710. *See* David Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769, 789 (2009).

12. *See* Seaman, *supra* note 2, 323.

13. *See id*.

14. *See id*.

15. Vickery v. Welch, 36 Mass. (19 Pick.) 523, 525-27 (1837).

16. *See* Seaman, *supra* note 2, 325.

17. *See id*.

opportunity to obtain an advantage over competitors who do not know or use it."[18]

The *Restatement* requires that "the subject matter of a trade secret must be secret."[19] Since practical considerations militate against a requirement for absolute secrecy, the *Restatement* offers relatively modest guidance as to where best to draw the line: "A substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the [relevant] information."[20] Although it emerged in subsequent years as an important resource for academic inquiry, the *Restatement* largely failed in its attempt to bring consistency and uniformity to the law of trade secrecy at the state level.[21]

B. *The Uniform Trade Secrets Act*

By the late 1960s, the Uniform Law Commission (ULC) sought to resurrect the project of uniformity—an effort that culminated with the development of the Uniform Trade Secrets Act (UTSA). By its own terms, this novel effort suffered from no shortage of ambition: "The contribution of the Uniform Act is substitution of unitary definitions of trade secret and trade secret misappropriation, and a single statute of limitations . . . The Uniform Act also codifies the results of the better reasoned cases concerning the remedies for trade secret misappropriation."[22]

The UTSA follows the *Restatement*'s example in enumerating the wide range of information that could plausibly be entitled to trade-secret protection, including "a formula, pattern, compilation, program, device, method, technique, or process."[23] To qualify, the information must meet two requirements. First, it must derive "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."[24] And second, it must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[25]

Parties who learn of trade secrets with knowledge or reason to know that the information was acquired through "improper means" risk suit for misappropriation. The UTSA defines these "improper means" to include "theft, bribery, misrepresentation, breach or inducement of a breach of duty to

18. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (Am. Law Inst. 1939).
19. *Id*.
20. *Id*.
21. *See* Seaman, *supra* note 2, 326.
22. Unif. Trade Secrets Act Prefatory Note (amended 1985) [hereinafter UTSA]
23. *Id*. at § 1.
24. *Id*.
25. *Id*.

maintain secrecy, or espionage through electronic or other means."[26] Notably, the UTSA also outlines a number of "proper means," which include discovery by independent invention, discovery by reverse engineering, discovery under a license from the owner of the trade secret, observation of the item in public use or on public display, or obtainment from published literature.[27]

The primary remedy in cases of misappropriation is injunctive. According to the UTSA, "[a]n injunction shall be terminated when the trade secret has ceased to exist, but the injunction may be continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation."[28] Subsequent amendments have provided for "payment of a reasonable royalty" in rare cases—typically those in which the grant of a prohibitive injunction would be unreasonable.[29]

Likely on account of its stated ambition to achieve uniformity, the first iteration of the UTSA sought to displace "conflicting tort, restitutionary, and other law . . . pertaining to civil liability for misappropriation of a trade secret."[30] More recent amendments clarified the scope of the UTSA's intended preemptive effect by exempting both contractual and criminal remedies from displacement.[31] The model statute provides for a three-year statute of limitations for all claims of trade-secret misappropriation.[32]

Within ten years of the UTSA's publication in 1979, more than 30 state legislatures had enacted the model statute in either its initial or amended form—albeit with some variation at the margins.[33] Although such rapid early success ensured that the pace of adoption would eventually slow, the reach and the appeal of the UTSA proved nothing less than remarkable. Once Texas—the nation's second-busiest docket for trade-secret litigation—enacted the UTSA in 2013, only three holdout jurisdictions remained.[34]

Despite the model statute's widespread adoption, individual states often amended the UTSA for idiosyncratic reasons. Variations among statutes of limitation offer perhaps the most visible example of these discrepancies. Although the model statute provides for a three-year statute of limitations, a sizeable minority of jurisdictions—including commercial hubs like Georgia, Illinois, and Ohio—have departed from this arrangement.[35] In place of the

26. *Id*.
27. *Id*.
28. *Id*. at § 2.
29. *Id*.
30. *Id*. at § 7.
31. *Id*.
32. *Id*. at § 6.
33. *See* Seaman, *supra* note 2, 391-92.
34. The three holdout jurisdictions are New York, Massachusetts, and North Carolina. *See id*. at 353.
35. *See id*. at 393-94.

model statute's provisions, one state—Alabama—adopted a two-year statute of limitations, while several others adopted four- and five-year statutes.[36]

At the same time, many jurisdictions have offered only lukewarm approval for Section Eight of the UTSA, which provides that the statute "be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this [Act] among states enacting it."[37] Several states, including Illinois and Pennsylvania, chose not to adopt Section Eight in any form.[38] Others have seen their courts effectively bypass Section Eight's mandate for uniformity through the adoption of minority positions.[39]

C. *The Economic Espionage Act of 1996*

During the 1990s—amid heightened fears of state-sponsored economic espionage—Congress took a cautious first step towards a federal law of trade secrecy. The Economic Espionage Act—which would eventually serve as the foundation for the DTSA—offered the promise of federal jurisdiction over the *criminal* consequences that might result from the theft of trade secrets. The EEA sought to criminalize two strains of theft: 1) industrial espionage on behalf of "any foreign government, foreign instrumentality, or foreign agent"[40] and 2) any theft of trade secrets for monetary gain.[41]

Unlike its civil counterparts, the EEA required a demonstration of unlawful intent—a *mens rea* of purpose or knowledge.[42] The EEA also criminalized both attempt and conspiracy.[43] Most ambitiously, the EEA purported to apply even to extraterritorial conduct—so long as: 1) the offender is "a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the law of the United States;" or 2) an "act in furtherance of the offense was committed in the United States."[44]

Upon its passage, the EEA met with heavy scholarly criticism for its putative breadth.[45] Unlike its state criminal counterparts, the EEA adopted the UTSA's relatively broad definition of what constitutes a trade secret—one that included "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques,

---

36. *See id.* at 393.
37. *See* Almeling, *supra* note 11, 774-75.
38. *See id.* at 775 n.21.
39. *See id.* at 775 n.22.
40. 18 U.S.C. § 1831 (2016).
41. 18 U.S.C. § 1832 (2016).
42. *Id.*
43. *Id.*
44. 18 U.S.C. § 1837 (1996).
45. *See generally* Robin Effron, *Trade Secrets, Extraterritoriality, and Jurisdiction*, 51 WAKE FOREST L. REV. 765, 768 (2016).

processes, procedures, programs, or codes."[46] According to Adam Cohen—formerly a lecturer at Yale Law School— "[t]his definition drew within it a wide range of mundane business information, including advertising plans, customer lists, and personnel information."[47]

Moreover, the EEA offered no express protection for reverse engineering, which the Supreme Court has defined as "starting with [a] known product and working backwards to divine the process which aided in its development or manufacture."[48] This omission is significant, as the UTSA—much like every state-level trade secret law—expressly protects reverse engineering.[49] Given the heavy criminal penalties that attach to conviction under the EEA[50], the omission of express protection for reverse engineering proved the subject of pointed scholarly criticism.[51]

The EEA included a jurisdictional requirement that attracted little notice upon its passage, but one that ultimately would play an outsized role in narrowing its scope. Any trade secret subject to the EEA must be "related to or included in a product that is produced for or placed in interstate or foreign commerce."[52] Facially far narrower than the Lanham Act's jurisdictional assertion, which includes "all commerce [that] may be lawfully regulated by Congress,"[53] this provision left open for more than 15 years serious questions as to the full extent of the EEA's reach.

As a practical matter, the deepest scholarly fears regarding the EEA—at least as they pertain to overbreadth—have not materialized. For reasons still not entirely clear, the statute has yielded only a trivial number of criminal prosecutions. A 2012 study counted only 124 criminal prosecutions since the EEA was passed in 1996—an average of fewer than 10 indictments per year.[54] Despite these shortcomings, however, the EEA would prove foundational to the passage of subsequent federal legislation.

D. *The Defend Trade Secrets Act of 2016*

During the 1990s and the 2000s, the drumbeat for expanding federal trade-secret protections accelerated. Various trade groups, including the American Intellectual Property Law Association and the Intellectual Property Owners Association, advocated for the creation of a civil cause of action under existing frameworks of the EEA.[55] Large corporate entities, too, including 3M,

46. 18 U.S.C. § 1839(3) (2016).
47. *See* Cohen, *supra* note 6, 204.
48. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).
49. *See* Cohen, *supra* note 6, 205.
50. *See* 18 U.S.C. § 1832(a)(5).
51. *See generally* Cohen, *supra* note 6, 205.
52. *See* Cohen, *supra* note 6, 206.
53. 15 U.S.C. § 1127 (2006).
54. *See* Seaman, *supra* note 2, 334 n.102.
55. *See id*. at 340 n.143.

Caterpillar, DuPont, GE, Eli Lilly, Microsoft, Monsanto, Philips, Procter & Gamble, and United Technologies all expressed support for expanding the reach of the EEA.[56]

In recent years, the problem of trade-secret misappropriation has received increased attention from public authorities as well. In February 2013, a White House-sponsored task force issued a report finding that the pace of industrial espionage and trade-secret theft was "accelerating."[57] Also in 2013, another report—this one issued by the United States Trade Representative—expressed similar concerns regarding "the apparent growth" of trade-secret misappropriation by foreign sources.[58]

In a remarkable testament to the interest and attention that federal protections for trade secrecy attracted, the six years prior to the DTSA's eventual enactment in 2016 witnessed no fewer than four discrete efforts to pass federal trade-secret legislation that incorporated a private cause of action.[59] Moreover, each proposal attracted at least nominal bipartisan support—no small feat in a period of extraordinary political polarization. The proposal that would eventually win passage—the Defend Trade Secrets Act—was first introduced in the 112th Congress, reintroduced in the 113th Congress, and then finally passed by the 114th Congress.[60]

In May 2016, President Obama signed this legislation, which was styled the Defend Trade Secrets Act of 2016.[61] The DTSA incorporates a private cause of action within the EEA, and it grants civil jurisdiction to any owner of a "trade secret that is misappropriated . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."[62] The DTSA also addresses prior criticisms of the EEA by clarifying that "improper means" do not include "reverse engineering, independent derivation, or any other lawful means of acquisition."[63]

In comparative terms, the DTSA appears to broaden the range and the scope of the remedies afforded by the UTSA. In addition to the injunctive remedy and reasonable royalties that characterize the UTSA's model statute, the DTSA offers two additional remedies. In cases of willful or malicious misappropriation, courts may award exemplary damages double the plaintiff's compensatory damages.[64] More controversially, courts also may order *ex parte*

---

56. *See id*. at 343.

57. *See id*. at 339 n.135.

58. *See id*. at n.139.

59. *See id*. at 340-41.

60. *See id*. at 341.

61. *See* S. 1890 Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016).

62. 18 U.S.C. § 1836(b)(1) (2016).

63. 18 U.S.C. § 1839(6)(B) (2016).

64. 18 U.S.C. § 1836(b)(3)(C) (2016).

seizures of any property used in the course of misappropriation should such a seizure prove necessary to prevent "irreparable harm."[65]

Perhaps most notably—at least with respect to its significance for the values of federalism—the DTSA includes an express anti-preemption provision.[66] As a practical matter, then, private plaintiffs may sue under both the state and the federal cause of action—an arrangement that demands additional inquiry into the scope and the scale of the new federal protections. In light of the lingering uncertainty surrounding the EEA's jurisdictional element, this exercise presents a novel challenge that implicates not only questions of statutory construction but also federalism.

PART TWO: THE JURISDICTIONAL ELEMENT

The Defend Trade Secrets Act provides a federal forum for claims of misappropriation "if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."[67] In a working paper that examines the jurisdictional element in extraordinary detail, Conor Tucker identifies two discrete requirements for proper jurisdiction.[68] This first is one of commerce—that is, the trade secret must be "used in, or intended for use in, interstate or foreign commerce."[69] The second is one of relatedness—that is, the trade secret must be "related to a product or service" that clears the hurdle set out by the commerce requirement.[70]

Although the DTSA defines several of its core[71] terms, the statute remains silent as to the bulk of the jurisdictional element, which was drawn from the criminal-theft provision of the EEA.[72] For instance, the statute makes no effort to define the "related to" term, which appears to be *sui generis* within federal law.[73] At the same time, the statute fails to define other terms within the jurisdictional element—"interstate commerce," most notably—which other statutes have sought to define.[74] In the absence of express statutory guidance, both the commerce requirement and the relatedness requirement merit additional scrutiny.

65. 18 U.S.C. § 1836(b)(2)(A)(ii)(II) (2016).

66. 18 U.S.C. § 1838 (2016).

67. 18 U.S.C. § 1836(b)(1).

68. Conor Tucker, *Interstate Trade Secrets? A Principled Framework for Identifying Federal Trade Secrets*, 7-8 (May 22, 2017), https://ssrn.com/abstract=2991373.

69. 18 U.S.C. § 1836(b)(1).

70. *Id*.

71. 18 U.S.C. §§ 1839(3) ("trade secret"); 1839(4) ("owner); 1839(5) ("misappropriation"); 1839(6) ("improper means).

72. *See* 18 U.S.C. § 1832(a) (2016).

73. Tucker, *supra* note 68, at 25.

74. *See, e.g.,* 15 U.S.C. § 1127 (2006).

A. *The Commerce Requirement*

The commerce requirement—that a trade secret must be "used in, or intended for use in, interstate or foreign commerce"—implicates at least two serious questions regarding congressional prerogatives under the Commerce Clause. The first is the longstanding debate surrounding the constitutional scope of congressional regulation. The second is subtler and less well-examined—the extent to which Congress may choose to limit by statute the statutory scope of its regulatory activities somewhere short of its full constitutional authority.

1. *Constitutional Scope*

After a return to prominence in the 1990s and the 2000s, the former question—the full scope of permissible constitutional authority—now seems well-settled. In *United States v. Lopez*, the Supreme Court reiterated that Congress may regulate three "broad categories of activity" under its commerce power: 1) the channels of interstate commerce, 2) the instrumentalities of interstate commerce, or persons or things in interstate commerce, and 3) activities "having a substantial relation to interstate commerce, *i.e.*, those activities that substantially affect interstate commerce."[75]

As a constitutional matter, confusion and controversy persist most often within the third category—those activities, including purely intrastate endeavors, that substantially affect interstate commerce.[76] However, the commerce requirement of the DTSA's rather inelegant jurisdictional element, which was adapted verbatim from the EEA, appears to fall comfortably within the second category of activities. Indeed, Christopher Seaman, one of the DTSA's most vocal critics, has described the commerce requirement as "facially constitutional," and further observed it "falls short of the constitutional limit."[77]

2. *Statutory Scope*

The cost of this constitutional certainty manifests as jurisdictional uncertainty as to the true scope of the DTSA's commerce requirement. In *Jones v. United States*, the Supreme Court held that the words "used in" acted as "limiting language" with respect to Congress' statutory exercise of its commerce power.[78] Moreover, the statute at issue in *Jones*, a criminal prohibition against arson, contained a jurisdictional element that was, if anything, facially far broader than the DTSA's analogous provision: "Whoever

75. United States v. Lopez, 514 U.S. 549, 558-59 (1995) (internal citations omitted).
76. *See id.*
77. Seaman, *supra* note 2, at 350-51.
78. Jones v. United States, 529 U.S. 848, 857 (2000).

maliciously damages or destroys . . . by means of fire or an explosive, any building, vehicle, or other real or personal property used in interstate or foreign commerce *or in any activity affecting* interstate or foreign commerce."[79]

As the private residence destroyed by arson in *Jones* could not move within interstate commerce, the government instead argued that it was "used in" at least three activities *that affected* interstate commerce: 1) to obtain and secure a mortgage from an out-of-state lender, 2) to obtain a casualty insurance policy from an out-of-state underwriter, and 3) to receive natural gas from other out-of-state sources.[80] But the Court rejected this novel argument: "Were the Court to adopt the Government's expansive interpretation, hardly a building in the land would fall outside § 844(i)'s domain, and the statute's limiting language, 'used in,' would have no office. Judges should hesitate to treat statutory terms in any setting as surplusage."[81]

Because the DTSA's commerce requirement appears still narrower, given its omission of the "activity affecting" term, there is good reason to suspect that Congress has chosen to forebear from legislating to the full extent of its constitutionally permissible authority. Perhaps the most obvious point of comparison is the Lanham Act, which likewise sought to federalize trademark law on the basis of congressional authority under the commerce power.[82] At first glance, the Lanham Act appears to offer a comparably narrow jurisdictional element—it applies only to trademarks that are "use[d] in commerce."[83]

However, the Lanham Act offers a definition of "commerce" that belies such a narrow rendering: "The word 'commerce' means all commerce which may lawfully be regulated by Congress."[84] This definitional adjustment—which ensures the statutory scope of jurisdiction reaches the full extent of constitutionally permissible authority—resolves any jurisdictional uncertainty with respect to federal trademark law. The DTSA, by contrast, provides no definition of terms like "used in" or "interstate commerce" that might offer comparable insights.[85]

Title 18 of the United States Code—which houses the DTSA, an amendment to an already-existing criminal law—does offer a generalized definition for interstate commerce: "The term 'interstate commerce', as used in this title, includes commerce between one State, Territory, Possession, or the District of Columbia and another State, Territory, Possession, or the District of

79. 18 U.S.C. § 844(i) (2004) (emphasis added).
80. Jones, 529 U.S. at 848-49.
81. *Id*. at 849.
82. *See* 15 U.S.C. § 1125 (2012).
83. 15 U.S.C. § 1125(a)(1).
84. 15 U.S.C. § 1127.
85. *See* 18 U.S.C. § 1839.

Columbia."[86] To the extent courts might view this reference as useful for the purposes of the DTSA, it is facially narrow.

Moreover, Conor Tucker has observed that Title 18 of the United States Code runs rife with examples where Congress intends to provide a more expansive exercise of its commerce power through specific statutory inclusion of the term "affecting" prior to "interstate commerce."[87] By definition, then, such a pattern requires that the baseline provision for what constitutes "interstate commerce" in the statutory context fall somewhere short of the full scope of "interstate commerce" that is subject to constitutionally permissible regulation.

3. *Conclusions*

Perhaps in exchange for its virtually certain constitutionality, the DTSA's commerce requirement is ambiguous. Although it seems clear—necessary, even—that the meaning of "interstate commerce" within the statutory context falls somewhere short of the full scope of "interstate commerce" subject to constitutionally permissible regulation, the DTSA offers little evidence of where such a line may be drawn confidently.

B. *The Relatedness Requirement*

The jurisdictional element provides that the trade secret be "related to a product or service."[88] The plain meaning of this relatedness requirement offers few hints as to its scope. Indeed, it could be argued, relatedness is always defined by further reference to degrees of proximity. Moreover, the relatedness requirement, very much unlike the commerce requirement, is entirely novel within federal law, so there is no accumulated meaning on which to rely.[89]

1. *Principles of Construction*

Nonetheless, at least one background principle of statutory construction points toward an understanding of the relatedness requirement that serves to narrow the jurisdictional element of the DTSA. As Justice Ginsburg observed in *Jones*, "[j]udges should hesitate to treat statutory terms in any setting as surplusage."[90] Given that a broad reading of the relatedness requirement likely would obviate its need, this background principle would seem to point only in the direction of further narrowing. Put another way, to the extent that the relatedness requirement *must* be construed to have meaning, its sole logical

86. 18 U.S.C. § 10.
87. Tucker, *supra* note 68, at 24 n.156.
88. 18 U.S.C. § 1836(b)(1).
89. Tucker, *supra* note 68, at 25.
90. Jones 529 U.S. at 849.

consequence must be to narrow the reach of the DTSA's jurisdictional element.[91]

2. *Contextual Differences*

As Conor Tucker has observed, one major difference between the text of the EEA's economic-espionage provision and its criminal-theft provision, which served as the basis for the DTSA's jurisdictional element, likewise could argue in favor of some narrowing effect.[92] The EEA's criminal-theft provision contains the now-familiar requirements of commerce and relatedness that articulate the parameters of the DTSA's reach: "[R]elated to a product or service used in or intended for use in interstate or foreign commerce."[93]

But the EEA's economic-espionage provision contains no such qualification. Instead, it attaches to anyone who, "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent," misappropriates a trade secret in prescribed fashion.[94] For Tucker, this absence is significant.[95] Without additional context, however, there is an obvious explanation for the difference—and one that may not bear meaningfully on the scope of the DTSA's jurisdictional reach. Any misappropriate trade secret that crosses, or is meant to cross, a foreign border necessarily will be subject to federal jurisdiction—a revelation that renders superfluous the DTSA's commerce requirement, if not necessarily its requirement of relatedness.[96]

3. *The Anti-Preemption Provision*

Perhaps the strongest contextual argument for a narrow reading of the relatedness requirement comes in the form of the DTSA's novel anti-preemption provision. Section 1838 provides: "This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret."[97] Such anti-preemption

---

91. Tucker, *supra* note 68, at 25-26.

92. *Id*. at 28.

93. *See* 18 U.S.C. § 1832(a).

94. *See* 18 U.S.C. § 1831(a).

95. "Its [e]ffect is to narrow *which trade secrets* support an action for misappropriation: under the economic espionage provision of the EEA, *any* trade secrets support prosecution; under the DTSA, only *sufficiently related* trade secrets support civil action." *See* Tucker, *supra* note 68, at 28.

96. *See* 28 U.S.C. § 1332(a)(4) (2016).

97. One notable exception to the anti-preemption provision creates effective immunity for whistleblowers and others who disclose confidential information to the government. *See* 18. U.S.C. § 1838.

clauses are exceedingly rare among federal statutes, and by their own terms may be read as significant evidence of narrow statutory purpose.[98]

In a world of already-substantial overlap among state and federal law, the broader the reading of the federal statute, the greater the possibility that preemption-related issues will arise. Tucker emphasizes that a broad reading of the relatedness requirement, and of the DTSA's jurisdictional element more generally, could force the *de facto* federalization of wide swaths of the very state laws upon which the law of trade secrecy generally relies for enforcement.[99]

4. *Conclusions*

Indeed, such policy considerations appear to augment what otherwise remains a circumstantial case for the relatedness requirement's narrowing effect. As a purely logical matter, the background principles of statutory construction suggest *some* narrowing effect, too. But its scope remains to this point recondite. With no analogue or other point of meaningful comparison in federal law—outside, that is, of the criminal-theft provision of the EEA—the relatedness requirement presents a puzzle that admits of few definitive conclusions.

C. *The EEA's Jurisdictional Element in Practice*

Although the DTSA's jurisdictional element has yet to be tested at the appellate[100] level, two panels from the Second Circuit have addressed the questions raised by the commerce and relatedness requirements contained within the EEA's criminal-theft provision. Unfortunately, the results in *United States v. Aleynikov*[101] and *United States v. Agrawal*,[102] which were decided within a year of one another, appear to be at loggerheads. Moreover, Rosemary Pooler—the only judge to sit on both panels—joined the majority opinion in *Aleynikov*[103] and dissented on the crucial jurisdictional question in *Agrawal*.[104]

1. United States v. Aleynikov

In *Aleynikov*, the Second Circuit unexpectedly reversed the conviction of Sergey Aleynikov—a computer programmer accused of misappropriating

98. Run several different ways, a Westlaw search turned up less than a dozen instances of similar anti-preemption clauses in various federal laws.

99. Tucker, *supra* note 68, at 29-30.

100. A survey of civil actions filed under the DTSA likewise did not yield any relevant challenges to the statute's jurisdictional ambit.

101. United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

102. United States v. Agrawal, 726 F.3d 235 (2d Cir. 2013).

103. *See Aleynikov*, 676 F.3d at 71.

104. *See Agrawal*, 726 F.3d at 262 (Pooler, J., dissenting).

source code for high-frequency trading algorithms during a career transition from one financial institution to another.[105] Shortly before his departure from Goldman Sachs & Co., Aleynikov had uploaded more than 500,000 lines of source code to a server based in Germany.[106] Shortly thereafter, he was charged with—among other offenses—violating the EEA's criminal-theft provision and was eventually convicted.[107]

At the time, the jurisdictional element of the criminal-theft provision applied to anyone who intentionally converted a trade secret "*related to or included in a product that is produced for or placed in interstate or foreign commerce*" in the statutorily prescribed manner.[108] Relying in large part on the Supreme Court's analysis of the statutory scope of commerce-power enactments in *Jones v. United States*, the Second Circuit concluded, "Goldman's [high-frequency trading] system was neither 'produced for' nor 'placed in' interstate commerce. Goldman had no intention of selling its HFT system or licensing it to anyone. It went to great lengths to maintain the secrecy of its system"[109]

The Second Circuit's surprise decision in *Aleynikov* elicited no small measure of controversy.[110] Indeed, the opinion's parting words suggest unease at the consequences of reversal: "The conduct found by the jury is conduct that Aleynikov should have known was in breach of his confidentiality obligations to Goldman, and was dishonest in ways that would subject him to sanctions; but he could not have known that it would offend this criminal law or this particular sovereign."[111]

2. *The Congressional Response to* Aleynikov

Despite voting with the majority on account of the "strength of [its] analysis of the text and the legislative history," Judge Guido Calabresi wrote separately to suggest that Congress revisit the EEA: "While concurring, I wish to express the hope that Congress will return to the issue and state, in appropriate language, what I believe they meant to make criminal in the EEA."[112] Shortly thereafter, Congress granted Judge Calabresi's wish by passing the Theft of Trade Secret Clarification Act of 2012 (TTSCA), which

105. *Aleynikov*, 676 F.3d at 82.

106. *Id*. at 74.

107. *Id*. at 75-76.

108. *See id*. at 79 (emphasis added).

109. *Id*. at 82.

110. According to one commentator, "[t]he consensus was not so much that the Second Circuit's ruling in *United States v. Aleynikov* was wrong—although there were certainly commentators who believed that—but rather that there was something amiss with a trade secrets legal regime that could offer up no law that Aleynikov had violated."

Cohen, *supra* note 6, at 190.

111. *Aleynikov*, 676 F.3d at 82.

112. *Id*. at 83 (Calabresi, J., concurring).

amended the EEA's jurisdictional element to its current form by clarifying that a product must be "used in *or intended for use*" in interstate commerce.[113]

Upon the TTSCA's passage by the upper chamber, Senator Patrick Leahy—the amendment's principal author and then-Chairman of the Senate Judiciary Committee—noted, "The clarifying legislation that the Senate has passed today corrects the [*Aleynikov*] court's narrow reading to ensure that our federal criminal laws adequately address the theft of trade secrets related to a product or service used in interstate commerce."[114] Shortly thereafter, the Second Circuit faced the opportunity to revisit these same issues in a case with strikingly similar facts.

3. United States v. Agrawal

In *United States v. Agrawal*, the Second Circuit affirmed the conviction of Samarth Agrawal—a quantitative analyst employed by Société Générale, who printed proprietary source code for high-frequency trading algorithms onto thousands of sheets of paper in anticipation of his departure for another financial institution.[115] Although prosecutors sidestepped any difficulties with the commerce requirement by contending that the underlying securities—rather than the source code itself—constituted the "product" at issue, Agrawal relied on *Aleynikov* to argue for a narrow reading of the relatedness requirement as well.[116]

However, the majority proved unsympathetic to Agrawal's entreaties. Beginning with a plain-language analysis of the relatedness requirement, the majority opinion observes, "The ordinary meaning of *related to* is *broad*: to stand in some relation; to have bearing or concern; to pertain; refer; to bring into association with or connection with."[117] The consequences of this broad construction are predictable: "The use of so deliberately expansive a term as 'related to' hardly signals [restrictive] intent. Nor can it be inferred from the EEA's legislative history. Accordingly, we conclude that the term 'related to,' as used in the EEA's nexus provision, is intended to reach broadly, rather than narrowly, consistent with its usual meaning."[118]

Judge Pooler—the sole jurist to sit on both the *Aleynikov* and the *Agrawal* panels—dissented from her colleagues' broad reading of the EEA's jurisdictional element.[119] Although she was skeptical of the notion that the underlying securities, rather than the source code, satisfy the jurisdictional

113. Pub. L. No. 112-236, 126 Stat. 1627, Sec. 2 (2012).

114. Statement of Senator Patrick Leahy, Theft of Trade Secrets Clarification Act of 2012, S. 3642 (Nov. 27, 2012) a*vailable at* https://www.leahy.senate.gov/press/senate-approves-leahy-bill-to-address-trade-secret-theft.

115. *Agrawal*, 726 F.3d at 237.

116. *Id*. at 246-47.

117. *Id*. at 247.

118. *Id*. at 248

119. *Id*. at 262 (Pooler, J., dissenting).

element's commerce requirement,[120] Judge Pooler reserved her harshest criticisms for the majority's analysis of the relatedness requirement: "This reading of *related to* is also so stretched that it affronts Supreme Court precedent. [It] has previously affirmed that 'where *related to* is used in legislation creating a discrete exception to a general rule, it may not be construed so expansively as to swallow the general rule.'"[121]

4. *Conclusions*

Both the meaning and the significance of *Aleynikov* and *Agrawal* as they relate to the DTSA's jurisdictional element remain contested. On the one hand, the analysis in *Aleynikov* accords with the available statutory inferences that suggest a narrowing effect to both commerce and relatedness requirements. On the other hand, the powerful combination of the congressional response to *Aleynikov* and the Second Circuit's subsequent decision in *Agrawal* points to a far more permissive construction in the case of the DTSA—particularly given the background mandate that courts read criminal statutes more narrowly than their civil counterparts.

D. *Conclusions*

The DTSA's jurisdictional element presents a confluence of novel elements. The commerce requirement appears to confer jurisdiction that falls somewhere short of the constitutionally permissible horizon for regulation. Unique among federal statutory provisions, the relatedness requirement presents a definitional question of first impression. And an anti-preemption provision of still-elusive provenance looms large, if just offstage. These complexities offer courts tasked with interpreting and applying the DTSA no small measure of challenge.

PART THREE: THE VALUE (AND VALUES) OF FEDERALISM

In one sense—and entirely apart from the passage of the DTSA—the evolution of the law of trade secrecy at the state level offers a remarkable study in the mechanics of horizontal federalism. And given the swirling uncertainties that surround the DTSA's jurisdictional ambit, it seems quite likely that the next chapter in the evolution of trade-secret law will offer its own grand experiment in vertical federalism. Indeed, the DTSA's novel anti-preemption provision suggests that, where possible, plaintiffs will avail themselves of all remedies under *both* state and federal law. So, it seems appropriate to ask how the values of Our Federalism may inform the DTSA, and *vice versa*.

120. *Id*. at 265-67 (Pooler, J., dissenting).
121. *Id*. at 268 (Pooler, J., dissenting).

A. *The Illusory Choice Between Uniformity & Experimentation*

Federalism is sometimes framed as a choice between uniformity, on the one hand, and policy experimentation on the other.[122] But this trope likely traffics in oversimplification. And as applied to the DTSA and the law of trade secrecy, it is particularly inapt. Indeed, the long march of the UTSA from one jurisdiction to the next has harmonized the substantive law of trade secrecy to an extraordinary degree.[123] It is significant that—prior to the passage of the DTSA in 2016—all but three states shared a common statutory understanding of what information constitutes a "trade secret" and what behavior constitutes "misappropriation."[124]

Moreover, the substantive differences among the handful of states that still adhere to the *Restatement* and the clear majority of jurisdictions that have enacted the UTSA are modest and, to a significant degree, marginal. Again, both the *Restatement* and the UTSA concur in the central qualifying requirements for trade-secret protection: 1) the underlying information retains its value because it is not generally known or used by competitors;[125] and 2) the owner must take affirmative steps to keep the underlying information secret.[126]

Perhaps more significantly, the DTSA's novel anti-preemption provision virtually ensures that the ready availability of a federal forum will undermine—rather than bolster—any ambition towards uniformity. As a practical matter, enforcement will appear in the form of a "two-tiered" system—where some claims may be filed under both the DTSA and the applicable state law, some claims may be filed only under the applicable state law, and, in rare cases, some claims may be filed only under the DTSA.[127] Accordingly, the broader the jurisdictional reach of the DTSA, the greater the possibility for divergence between federal and state law.

Moreover, the availability of a federal forum will not alter the reality that claims of misappropriation often implicate embedded questions of state law. According to Christopher Seaman, "[t]rade secret claims and allegations are closely intertwined with contracts, such as employment contracts and joint-venture agreements that are governed by state law."[128] Indeed, there is often no federal analogue to the state laws that govern fiduciary duties, as well as the scope and enforceability of restrictive covenants like non-disclosure

122. *See, e.g.*, *Laboratories of Democracy? Brandeis, Federalism, and Scientific Management*, 31 PUBLIUS: THE JOURNAL OF FEDERALISM, 37 (Winter 2001).

123. *See* Seaman, *supra* note 2, at 353-54.

124. *See id*. at 354-55.

125. *See id*. at 356 n.264.

126. *See id*. at 356 n.265.

127. Given the close *substantive* resemblance between the DTSA and the UTSA's model statute, it is difficult to imagine a circumstance in which a claim could be filed under the DTSA, but not the applicable state law.

128. *See* Seaman, *supra* note 2, at 364 (internal quotation marks omitted).

agreements and non-compete clauses.[129] As a practical matter, then, a narrow reading of the DTSA's jurisdictional element appears best suited to the interests of uniformity.

By the same token, a narrow reading of the DTSA's jurisdictional element will serve another core value of federalism—policy experimentation.[130] Given the widespread adoption of the UTSA, it is true that broad consensus has developed around the core concerns of the law of trade secrecy. But at the margins, there remain no small number of unsettled issues—open questions that courts, legislatures, and polities have yet to answer definitively, and questions for which there may not be an obvious or uniform answer. An example will prove illustrative.

B. *Case Study: Inevitable Disclosure*

The doctrine of so-called "inevitable disclosure" remains one of the most controversial flashpoints within the law of trade secrecy. In 1995, the Court of Appeals for the Seventh Circuit affirmed a temporary injunction against a PepsiCo executive, William Redmond, Jr., who was poised to take on a nearly identical role with a direct competitor.[131] By way of his tenure with PepsiCo, Redmond was privy to various trade secrets—information on which, absent "an uncanny ability to compartmentalize," he would necessarily rely in his new role.[132]

The Seventh Circuit's conclusion that "a plaintiff may prove a claim of trade secret misappropriation by demonstrating that [a] defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets" has met with no small measure of controversy.[133] Several years after the Seventh Circuit's decision in *PepsiCo*, a California appellate court took up a similar request from a company that specialized in hardware locks.[134] Although the court acknowledged that "the majority of jurisdictions addressing the issue have adopted some form of the inevitable disclosure doctrine," it pointedly declined to do so—and then engaged in a blistering doctrinal critique.[135]

According to the court, "The decisions rejecting the inevitable disclosure doctrine correctly balance competing public policies of employee mobility and protection of trade secrets. The inevitable disclosure doctrine permits an employer to enjoin the former employee without proof of the employee's actual or threatened use of trade secrets based upon [circumstantial] inference."[136]

129. *See id*.

130. *See generally* Michael Dorf and Charles Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267 (1998).

131. PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1263-64 (7th Cir. 1995).

132. *Id*. at 1269.

133. *Id*.

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

135. *Id*. at 1460-61.

136. *Id*. at 1461-62.

When pressed, the court casts its lot decisively in favor of autonomy and mobility: "The chief ill in the covenant not to compete imposed by the inevitable disclosure doctrine is its after-the-fact nature: The covenant is imposed *after* the employment contract is made and therefore alters the employment relationship without the employee's consent."[137]

Amid concerns that the DTSA would offer enterprising plaintiffs a collateral means of introducing the doctrine of inevitable disclosure to jurisdictions that—much like California—studiously had avoided its adoption, Senator Dianne Feinstein successfully introduced an amendment proscribing any injunction that would "prevent a person from entering into an employment relationship."[138] Her concerns were vindicated within a month of the DTSA's enactment when Judge Jon Tigar of the Northern District of California ruled on one of the first suits filed under the auspices of the DTSA—and one whose factual posture otherwise would have offered a textbook opportunity for resort to inevitable disclosure.[139]

It is, of course, significant that, for the purposes of the DTSA, this controversy was resolved in favor of policy experimentation. Although the doctrine of inevitable disclosure presented an issue so controversial that the DTSA was amended prior to passage to address it expressly, the example nonetheless offers insight into the enduring significance of state-by-state experimentation. Indeed, the recency of the controversy surrounding inevitable disclosure—recall that *PepsiCo* was decided only in 1995—serves to underscore the relative youth and dynamism that characterize the modern law of trade secrecy.

But the flexibility afforded by the opportunity for policy experimentation also reflects diversity among regional interests. In California—where, for instance, software companies are highly concentrated and trade secrets related to software development are known to be ephemeral—a strong policy against the doctrine of inevitable disclosure likely makes good sense. By the same token, in jurisdictions where more traditional industrial interests still predominate—and whose trade secrets may, if protected, continue to generate value for decades—the security afforded by the doctrine of inevitable disclosure may outweigh the public interest in employee mobility that jurisdictions like California have prioritized.

PART FOUR: CONCLUDING OBSERVATIONS

In the coming years, the law of trade secrecy is likely to meet with increasing prominence and scrutiny. As the patent system continues to strain under the weight of a profusion of litigation—to say nothing of the other downsides that characterize a one-size-fits-all regime for protection and

137. *Id*. at 1462-63.
138. *See* 18 U.S.C. § 1836(b)(3)(A)(i)(I).
139. *See* Henry Schein, Inc. v. Cook, 191 F. Supp. 3d 1072 (N.D. Cal., 2016).

enforcement—it seems likely that profit-seekers in sectors ranging from software to pharmaceuticals will turn increasingly to the law of trade secrecy for relief. Unlike its thoroughly federalized patent counterpart, the law of trade secrecy offers an enviable degree of dynamism and flexibility.

It is, of course, no coincidence that these virtues mirror the benefits of which federalism's proponents so frequently speak. Indeed, the evolution of the law of trade secrecy has—to this point, at least—offered a remarkable case study in federalism at its best. And if properly—which is to say, narrowly—construed, there is little reason that the DTSA cannot provide a similarly compelling next chapter to this story. By providing on the one hand a federal forum and an absolute floor for the protection of trade secrets, and on the other ample space for policy experimentation around still-contested or emerging questions, a narrowly construed DTSA will help to ensure the law of trade secrecy is well-positioned for a dynamic, if uncertain, future.