LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Intellectual Property Litigation Practice April 18, 2016 | Number 1954

5 Things to Know About the Defend Trade Secrets Act

Unanimous Senate approval of the federal trade secrets bill creates momentum for a new cause of action.

After nearly a year-long delay, the Senate on April 4, 2016, unanimously passed the Defend Trade Secrets Act (DTSA), which now awaits approval by the House of Representatives. The bill's strong bipartisan support reflects broader concern over trade secret theft across industry sectors. As former Attorney General Eric Holder put it, "[t]here are only two categories of companies affected by trade-secret theft: those that know they've been compromised and those that don't know yet.'' If enacted, the DTSA will create a new federal cause of action in addition to those available under state trade secret laws. The DTSA will provide businesses with novel avenues for protecting their valuable competitive information, but may also create new pitfalls for the unwary. Here are five things businesses should know about the federal trade secrets bill.

1. The DTSA has broad political and business support.

Following the Senate Committee on the Judiciary's recommendation, the Senate passed the DTSA without opposition, 87-0.[1] The bill now heads to the House where it similarly enjoys broad support.[2] Rep. Bob Goodlatte, Chairman of the House Judiciary Committee, released a statement recognizing the importance of trade secrets and indicating his desire to move the bill forward "in the coming weeks."[3] The Obama Administration publicly supports the bill and "mitigating and combating the theft of trade secrets."[4] Businesses in traditionally innovative fields, including software, hardware, biotech, pharma, automotive and aerospace, have backed the DTSA, and players in less technology-focused industries such as manufacturing, fragrances, sporting goods and apparel have voiced their support as well.[5]

Whether a simple customer list or a highly complex block of computer code, trade secrets are among the most valuable competitive advantages that drive business success in every industry, which explains the overwhelming support for the DTSA. One 2013 estimate indicates that trade secret theft costs American businesses over US$300 billion annually; a 2014 estimate calculated the cost at almost US$500 billion.[6] The strong desire for a federal private cause of action to help stem trade secret theft, especially by foreign actors, has lent the DTSA significant momentum.

2. It would create a uniform nationwide law with international implications.

Of the four traditional forms of intellectual property — patents, copyrights, trademarks and trade secrets — only trade secret rights have been enforced exclusively through state laws. The DTSA would change that, but would not displace the existing state law trade secret regimes. Rather, the new federal rights would exist in parallel. The DTSA would afford some of the same benefits already available under patent, copyright and trademark laws: it would create a single, unified body of law that businesses and practitioners alike can become accustomed to and develop expertise in, instead of having to navigate the

nuances that differentiate the patchwork of trade secret regimes. The broad discovery tools available in federal court would be available in any action in which a federal trade secret claim is brought. For example, the federal subpoena power extends across state lines, unlike the subpoena authority of state courts.

The DTSA's reach would extend not only across state lines, but potentially also would apply to conduct beyond the nation's borders.[7] The DTSA contemplates the theft of trade secrets "used in, or intended for use in, interstate *or foreign* commerce."[8] A key concern for DTSA drafters was foreign industrial espionage.[9] The Economic Espionage Act (EEA), which the DTSA would amend, expressly states that its provisions "appl[y] to conduct occurring outside the United States" under specific circumstances.[10] Specifically, the EEA applies if the trade secret thief is a US-based entity, or if some part of the theft occurred within the US[11] The Federal Circuit has previously stated that this section may apply to foreign conduct.[12] The DTSA also would require the Attorney General, in consultation with other agencies, to provide future reports on trade secret theft "occurring outside of the United States" and recommendations on reducing the impact of such theft.[13]

3. It would grant trade secret owners the right to obtain ex parte seizures.

Among the DTSA's most striking features is that it allows for ex parte seizure orders. Upon a successful application, a court can order federal marshals to seize "property necessary to prevent the propagation or dissemination" of the stolen trade secret.[14] This order to seize property is without notice to the accused thief.[15] The drafters felt that such extraordinary relief was necessary because trade secrets are unique in their dependency on secrecy, and the harm from misappropriation may be mitigated if swift action is taken before a stolen trade secret is widely disseminated.[16]

The drafters were also aware of the potential for abuse of this new seizure remedy, limiting its availability to "extraordinary circumstances."[17] For example, any successful applicant would be required to provide security sufficient to cover damages for wrongful or excessive seizure.[18] The DTSA would also provide for a "seizure hearing," at which the party that obtained the order bears the burden to show that the order was necessary.[19] Further, victims of wrongful seizure may be entitled the same relief as available for an improper seizure under trademark law: a damages award, punitive damages for bad faith, and attorneys' fees.[20]

4. As patent protection has narrowed, trade secrets are likely to expand.

With the passage of the American Invents Act and in view of a number of Supreme Court decisions in recent years,[21] patent protection for some forms of intellectual property has narrowed. While the changing law on patent eligibility has particularly impacted sectors like software and medical diagnostics, it also has affected many other industries. For businesses working in fields where broad patent protection for their innovations is no longer as certain, trade secret protection may provide a better alternative. Trade secrets, unlike patents, can be maintained indefinitely so long as there are reasonable efforts to keep them secret. Also, unlike with patents, a trade secret owner need only take reasonable steps to protect the information; no lengthy application or prosecution process is necessary. In view of the quickly changing patent laws, trade secret protection is an increasingly attractive option for many companies, and the DTSA would provide a viable new platform for enforcing those rights.

5. Businesses should be inventorying and protecting trade secrets now.

Companies can move now to avail themselves of the trade secret protection framework under existing state laws, as well as to prepare for the DTSA. Systematically identifying confidential information that merits protection as a trade secret is a prudent, and often overlooked, step in maintaining a protectable

trade secret portfolio. To qualify as a trade secret, the information must derive its value from being generally unknown to the public.[22] Once identified, the intellectual property must also be the subject of reasonable measures to maintain its secrecy.[23] These measures can include physical locks, security guards, access control, confidentiality agreements and document labeling.[24] The law requires reasonable, rather than impenetrable, security measures.[25] Establishing an organized and well-documented trade secret inventory and standard protective measures will help prepare a company to enforce its rights when necessary.

The DTSA also would provide protection for certain "whistleblower" employees, and obligate employers to notify their workers of these protections.[26] For example, an employee who discloses a trade secret "solely for the purpose of reporting or investigating a suspected violation of law" would be protected from liability.[27] The DTSA would require employers to inform their employees of the various immunities available under the new law.[28] Failure to do so could deprive the employer of any right to punitive damages or attorneys' fees in an action against that employee.[29] "Employee" is defined broadly under the act, and sweeps in contractors and consultants.[30] Businesses can prepare by reviewing and standardizing their confidentiality, hiring and consulting agreements with an eye toward spelling out responsibilities regarding trade secret information. Should the DTSA become law, those businesses will be well-positioned to promptly implement the needed changes and benefit from new federal protections.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Gabriel S. Gross
gabe.gross@lw.com
+1.650.463.2628
Silicon Valley

Matthew W. Walch
matthew.walch@lw.com
+1.312.876.7603
Chicago

Nicholas H. Yu
nicholas.yu@lw.com
+1.650.463.2697
Silicon Valley

You Might Also Be Interested In

PTO Issues New Final Rules for PTAB Proceedings (March 31, 2016)

New Game Plan: Federal Circuit Decision May Revive "Redskins" Trademarks

The Latest on PTAB

Combating Online Anonymous Defamation

---

jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's *Client Alerts* can be found at www.lw.com. If you wish to update your contact details or customize the information you receive from Latham & Watkins, visit http://events.lw.com/reaction/subscriptionpage.html to subscribe to the firm's global client mailings program.

Endnotes

1 *See* http://www.reuters.com/article/us-usa-trade-secrets-idUSKCN0X11Y3.

2 *See* https://www.congress.gov/bill/114th-congress/house-bill/3326/cosponsors (listing Democrat and Republican sponsors).

3 Statement of Rep. Bob Goodlatte (R-Va.), *available at* https://judiciary.house.gov/press-release/goodlatte-applauds-senate-passage-trade-secrets-legislation/.

4 *See* https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saps1890s_20160404.pdf.

5 *See* http://www.reuters.com/article/us-usa-trade-secrets-idUSKCN0X11Y3; http://www.ipwatchdog.com/2016/04/04/obama-administration-supports-defend-trade-secrets-act/id=67993/; http://www.bloomberg.com/politics/articles/2016-04-04/senate-set-to-pass-bipartisan-measure-to-protect-trade-secrets.

6 S. Rep. No. 114-220, at 2 (2016).

7 The Defend Trade Secrets Act, S. 1890, 114th Cong. § 2 (2016).

8 *Id.*

9 *See* http://www.hatch.senate.gov/public/_cache/files/a78f2d4c-1556-44fc-b3aa-f2b11d58b929/Hatch-Coons%20Trade%20Secrets%20Colloquy,%20October%208,%202015.pdf; *see also* https://dougcollins.house.gov/uploads/Defend%20Trade%20Secrets%20Act%20one-pager%20July%2029%202015.pdf.

10 18 U.S.C. § 1837.

11 *Id.*

12 *TianRui Grp. Co. v. Int'l Trade Comm'n*, 661 F.3d 1322, 1330 n.4 (Fed. Cir. 2011).

13 *Supra* note 7, § 4(b) (section titled "REPORT ON THEFT OF TRADE SECRETS OCCURRING ABROAD"). *See also id.* § 5(2) (noting the harmfulness of trade secret theft "wherever it occurs").

14 *Id.*

15 *Id.* § 2.

16 Senators Hatch and Coons, Colloquy on the Defend Trade Secrets Act, at 4, http://www.hatch.senate.gov/public/_cache/files/a78f2d4c-1556-44fc-b3aa-f2b11d58b929/Hatch-Coons%20Trade%20Secrets%20Colloquy,%20October%208,%202015.pdf.

17 *Supra* note 7, § 2.

18 *Id.*

19 *Id.*

20 *Id.* (allowing the same relief as provided in 15 U.S.C. 1116(d)(11)).

21 *See, e.g.*, *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014); *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289 (2012).

22 18 U.S.C. § 1839.

23 *Id.*

24 *See United States v. Chung*, 659 F.3d 815, 826 (9th Cir. 2011).

25 *See id.* at 827 (finding sufficient: signed confidentiality agreements with employees, employee training regarding confidentiality, confidentiality labeling of documents, and security guards that were empowered to search employee belongings and check ID).

26 *Supra* note 7, § 7.

27 *Id.*

28 *Id.*

29 *Id.*

30 *Id.*