SEVEN REASONS WHY TRADE SECRETS ARE INCREASINGLY IMPORTANT

David S. Almeling[†]

ABSTRACT

As technology reshapes the way we live and work, propelling the American economy toward one based on informational assets, trade secrets have never been more important. The ascent of the importance of trade secrets has unleashed an unprecedented boom in litigation, in legislation, and in media and scholarly attention. It has produced damages awards in the hundreds of millions of dollars, and prompted federal authorities to pursue aggressive criminal investigations. The author, an experienced trade secrets litigator, identifies seven factors behind this phenomenon: (1) digital technology; (2) a mobile workforce; (3) the rising value of intellectual property, of which trade secrets are a part; (4) the widespread adoption of the Uniform Trade Secrets Act; (5) trade secrets' flexible definition; (6) an increase in international threats; and (7) the shifting calculus between whether to pursue patent or trade secret protection. Whether each of these factors will continue to fuel trade secret growth remains uncertain; societal norms fluctuate, political winds shift. But taken together, these seven trends suggest that the business of trade secrets will only assume greater importance in the years ahead.

† David S. Almeling is a Counsel at O'Melveny & Myers LLP in the firm's San Francisco office. The opinions expressed in this article do not necessarily reflect the views of O'Melveny or its clients, and it should not be relied upon as legal advice.

TABLE OF CONTENTS

I. INTRODUCTION

The business of trade secrets—developing them, protecting them, stealing them, litigating them—is booming.

Examples of the boom include:

Litigation. Over the past three decades, trade secret litigation in federal courts has grown exponentially, doubling roughly every decade, while federal litigation has decreased overall.[1] And over the past two decades, trade secret litigation in state courts has increased at a rate faster than that of state litigation in general.[2]

Legislation. No legislation prohibiting trade secret misappropriation existed before 1980. Today, forty-seven states have a civil statute and over

1. David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 293, 301–02 (2010) [hereinafter *Federal Study*].

2. David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 67–68 (2011) [hereinafter *State Study*]. While the growth in federal trade secret cases was exponential, the Administrative Office of the U.S. Courts reports that from 2000 to 2009, total civil filings decreased by two percent. Judicial Business of the United States Courts, ADMINISTRATIVE OFFICE OF THE U.S. COURTS, 11 (2009), *available at* http://www.uscourts.gov/Statistics/JudicialBusiness/JudicialBusiness.aspx?doc=/uscourts/Statistics/JudicialBusiness/2009/JudicialBusinespdfversion.pdf.

half of those states also have specific criminal statutes.[3] In 1996, Congress passed a federal statute criminalizing trade secret misappropriation,[4] and in 2011 two senators introduced an amendment that, had it passed, would have provided a federal right of civil action.[5]

Media and Scholarly Attention. Only one article about trade secrets appeared in a major U.S. newspaper in the 1970s, but the number of articles on this topic has since mushroomed: 159 articles in the 1980s, 548 in the 1990s, and 593 in the 2000s.[6] Likewise, in the 1970s, there were twenty-six law review articles about trade secrets; by the 1980s that number had grown to 320 articles, by the 1990s to 1,105, and by the 2000s to 1,546.[7]

Value of Trade Secrets. Because of their confidential nature, it is difficult to accurately assess the value of trade secrets today or compare their current value to that of years past. But economists do value intangible assets, which include trade secrets and other types of intellectual property. The intangible assets of the 500 companies that make up the S&P 500 comprised 17 percent of the companies' total value in 1975, 32 percent of total value in 1985, 68 percent of total value in 1995, 80 percent of total value in 2005, and 81 percent of total value in 2009.[8]

---

3. *State Study*, *supra* note 2, at 75. New Jersey is the latest state to adopt the UTSA, enacting it on January 9, 2012. *See generally* New Jersey Trade Secrets Act (S-2456/A921).

4. Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–39 (2006).

5. David S. Almeling, *Guest Post: First Patent Reform, Now Trade Secret Reform?*, PATENTLY-O (Oct. 12, 2011), http://www.patentlyo.com/patent/2011/10/almeling-trade-secret.html.

6. I do not purport to have conducted a rigorous statistical analysis of citations in newspapers. Instead, I ran a series of searches in Westlaw's Major Newspapers (NPMJ) database, which contains more than four dozen of the most widely circulated daily U.S. newspapers, for the ten-year periods defined above. I required the article to use the phrase "trade secret" at least three times to increase the percentage of articles that were focused on trade secrets—e.g., for the 1970s, atleast3("trade secret!") & da(aft 12/31/1969 & bef 01/01/1980)—as opposed to articles that merely mentioned them in passing.

7. I also do not purport to have conducted a rigorous statistical analysis of citations in law review articles. Rather, I ran a series of searches in Westlaw's Journals and Law Reviews PRO, which contains all available law reviews and bar journals on Westlaw, for the ten-year periods defined above. I required the article to use the phrase "trade secret" at least five times to increase the percentage of articles that were focused on trade secrets—e.g., for the 1970s, atleast5("trade secret!") & da(aft 12/31/1969 & bef 01/01/1980)—as opposed to articles that only mentioned them in passing. I required the law review articles to use the phrase five times, but only three times for newspapers, because law review articles are typically longer.

8. James E. Malackowski, *The Intellectual Property Marketplace: Past, Present and Future*, 5 J. MARSHALL REV. INTELL. PROP. L. 605, 611 (2006); Press Release, Ocean Tomo, Ocean Tomo's Annual Study of Intangible Asset Market Value – 2010 (Apr. 4, 2011), *available at* http://www.oceantomo.com/media/newsreleases/intangible_asset_market_Value_2010.

Damages Awards. Trade secret awards now include headline-grabbing sums in the hundreds of millions of dollars, numbers unheard of decades ago. In 2011 alone, those awards included $947 million to medical device manufacturer St. Jude Hospital based on an employee's misappropriation of trade secrets,[9] $920 million to chemical company DuPont for trade secret misappropriation of its Kevlar fiber product,[10] and $525 million to hard disk drive manufacturer Seagate based on misappropriation by its rival Western Digital.[11]

Several factors help to explain this remarkable growth. One factor is the tectonic shifts in technology reshaping almost every aspect of American life. Trade secrets were once stored under lock and key in hard-copy form, making it difficult to both access and walk away with the protected information. The revolution in digital storage—cloud computing, e-mail, thumb drives—makes it easier to take trade secrets, whether the culprit is an employee who copies company secrets on a thumb drive or a hacker who breaches the company's network from thousands of miles away.

Another factor is the changing American workforce. Gone are the days of "the company man," devoting his career to a single employer. Today's workers are mobile, hopping from job to job—and, whether by design or accident, often taking their former employers' trade secrets with them.

In all, this Article advances seven factors that help explain why trade secrets have become so crucial to American businesses and their employees. Besides new technology and changes to the American workforce, those factors include the shift in corporate value from tangible to intangible assets, the Uniform Trade Secrets Act,[12] the expanding definition of what qualifies as a trade secret, the growth of international threats, and the changing balance between patent and trade secret law. Part II provides the context for the current growth by chronicling the history of trade secret law and its slow development vis-à-vis other forms of intellectual property. Part III presents the seven factors and also discusses countervailing evidence. Part IV

9. *St. Jude Trade Secret Theft Win Pared Back by $1.3 Billion*, MASSDEVICE (June 27, 2011), http://www.massdevice.com/news/st-jude-trade-secret-theft-win-pared-back-13-billion.

10. Jef Feeley et al., *Kolon Loses $920 Million Verdict to DuPont in Trial Over Kevlar*, BLOOMBERG BUSINESSWEEK (Sept. 15, 2011, 12:24 AM), http://www.businessweek.com/news/2011-09-15/kolon-loses-920-million-verdict-to-dupont-in-trial-over-kevlar.html.

11. Jacqueline Bell, *Seagate Wins $525M In Western Digital Secrets Row*, LAW360 (November 21, 2011, 1:06 PM), http://www.law360.com/ip/articles/287459?nl_pk=86604097-1f36-4bfa-a7ca96c7182cf1bc&utm_source=newsletter&utm_medium=email&utm_campaign=ip.

12. Uniform Trade Secrets Act (amended 1985), 14 U.L.A. 529 (2005).

concludes with a prediction: the same factors that underlie the boom in all things trade secret over the past few decades show no sign of abating and, thus, portend further increases in the development, misappropriation, and litigation of trade secrets.

II. THE SLUGGISH DEVELOPMENT OF TRADE SECRET LAW

Trade secret law in the United States is the newest and least developed of the "big four" types of intellectual property ("IP"): patents, copyrights, trademarks, and trade secrets.[13] Courts and legislatures embraced trade secret law last, and the federal government has yet to do so in the form of a civil statute. Trade secret law is thus the sole type of IP governed primarily by state law, a state of affairs I have lamented in previous articles.[14]

Patent law is the oldest of the big four. The custom of granting patents originated in Italy in the first half of the fifteenth century, and Venice enacted the first patent statute in 1474.[15] English courts recognized patents beginning in 1572, and England's parliament shaped patent law with the adoption of the Statute of Monopolies in 1623.[16] The American colonies continued in the English tradition, and almost all had granted patents by the time of the American Revolution.[17] With the adoption of the U.S. Constitution, the federal government assumed the power to grant patents,[18] and shortly thereafter, in 1790, Congress passed the first Patent Act.[19]

Modern copyright law enjoys a similarly long history. England's parliament enacted the first copyright statute with the Statute of Anne in 1710.[20] Shortly after its passage, courts recognized copyrights under common

13. *See, e.g.*, Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 315 (2008) (noting that "(t)rade secret law is a relative latecomer to the IP pantheon").

14. *See generally* David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769 (2009); David S. Almeling, *A Practical Case For Federalizing Trade Secret Law*, LAW360 (June 23, 2009), http://www.law360.com/articles/106724.

15. Edward C. Walterscheid, *The Early Evolution of the United States Patent Law: Antecedents*, 76 J. PAT. & TRADEMARK OFF. SOC'Y 697, 707–08 (1994).

16. *See, e.g.*, E. Wyndham Hulme, *The History of the Patent System Under the Prerogative and at Common Law*, 12 L.Q. REV. 141 (1896).

17. ARTHUR R. MILLER & MICHAEL H. DAVIS, INTELLECTUAL PROPERTY: PATENTS, TRADEMARKS, AND COPYRIGHT IN A NUTSHELL 7 (3d ed. 2000).

18. U.S. CONST. art. 1, § 8, cl. 8.

19. Patent Act of 1790, 1 Stat. 109 (codified as amended at 35 U.S.C. §§ 1–376 (2006)).

20. 8 Ann. c. 19, § 1 (1710) (Eng.).

law principles.[21] Copyright protection was authorized in the U.S. Constitution,[22] and Congress passed the Copyright Act in 1790.[23]

American trademark law has its origin in English common law, with the earliest pivotal English cases occurring in 1742[24] and 1824.[25] American courts first granted relief under trademark theories in 1837.[26] Congress enacted the first trademark statutes in 1870 and 1876, although the Supreme Court subsequently declared them unconstitutional.[27] Congress then passed the Trademark Act in 1881.[28]

While confidential business information is as old as business itself, trade secret law is a more recent phenomenon. The earliest American cases discussing trade secrets occurred in 1837[29] and 1868,[30] with the latter recognized as the first clear judicial statement of the law of trade secrets.[31] When the Restatement of Torts was published in 1939, it included a section summarizing the law of trade secrets.[32] The Restatement marks a critical turning point for trade secret law because before its publication, trade secret law had not yet "crystallized around any particular pattern."[33] The Restatement quickly became the legal standard, as nearly every reported trade secret case cited the Restatement.[34] But due to the nonbinding nature of the

21. *See, e.g.*, Millar v. Taylor, (1769) 98 Eng. Rep. 201, 217–19, 225–29 (K.B.); Donaldson v. Beckett, (1774) 1 Eng. Rep. 837 (H.L.).

22. U.S. CONST. art. 1, § 8, cl. 8.

23. Copyright Act of 1790, 1 Stat. 124 (codified as amended at 17 U.S.C. §§ 101–1332 (2006)) (copying almost verbatim the Statute of Anne).

24. Blanchard v. Hill, (1742) 26 Eng. Rep. 692 (Ch.).

25. Sykes v. Sykes, (1824) 3 B.& C. 541 (upholding a verdict against a manufacturer for appropriating another's mark on a stamp).

26. Thomson v. Winchester, 36 Mass. 214 (1887); *see* Daniel M. McClure, *Trademarks and Unfair Competition: A Critical History of Legal Thought*, 69 TRADEMARK REP. 305, 314 (1979).

27. United States v. Steffens, 100 U.S. 82 (1879) (*The Trade-mark Cases*).

28. Trademark Act of 1881, 21 Stat. 502 (1881); Trademark Act of 1881, Pub. L. No. 58-84, 33 Stat. 724, 727 (1905) (repealed by Lanham Act, § 46(a), Pub. L. No. 79-459, 60 Stat. 427, 444 (1946) (codified as amended in various sections of 15 U.S.C.)).

29. Vickery v. Welch, 36 Mass. (1 Pick.) 523, 524 (1837) (holding that there is an implied duty of confidentiality in shared trade secrets).

30. Peabody v. Norfolk, 98 Mass. 452, 457–58 (1868) (holding that one who invents and keeps secret a process of manufacture has a property right in it against one who in breach of confidence attempts to use it or disclose it to third persons).

31. Vincent Chiappetta, *Myth, Chameleon or Intellectual Property Olympian? A Normative Framework Supporting Trade Secret Law*, 8 GEO. MASON L. REV. 69, 70 (1999).

32. RESTATEMENT (FIRST) OF TORTS §§ 757–58 (1939).

33. William B. Barton, *A Study in the Law of Trade Secrets*, 13 U. CIN. L. REV. 507, 558 (1939).

34. Ramon A. Klitzke, *The Uniform Trade Secrets Act*, 64 MARQ. L. REV. 277, 282 (1980).

Restatement, trade secret law remained geographically inconsistent, developing unevenly from state to state.[35]

About forty years later, in an attempt to codify the common law of trade secrets and to promote uniformity, the Commissioners on Uniform State Law—the same folks who brought us the Uniform Commercial Code—drafted the Uniform Trade Secrets Act ("UTSA"). Following its adoption in 1979, the UTSA gained widespread acceptance, and as of late 2011, forty-seven states had enacted it in some form.[36] Despite the UTSA, trade secret law is still not uniform. Although only three states have not enacted it, those three (Massachusetts, New York, and Texas) represent 18 percent of the nation's GDP.[37] Further, states whose legislatures adopted it also modified it,[38] courts in different states interpreted it differently, and some courts continued to rely on common law even after their legislatures' enactment of the UTSA.[39]

Congress has made several attempts to bring trade secret law into the federal realm. In 1959, New York Representative John Lindsay introduced the Lindsay Bill, which sought to create a federal statutory cause of action,[40] but it went nowhere. And in 1966, Arkansas Senator John McClellan introduced the McClellan Bill, which sought to achieve the same goal by amending federal trademark law.[41] It was similarly unsuccessful. In 1996, Congress did pass the Economic Espionage Act and made misappropriation of trade secrets a federal crime, but that statute does not address civil misappropriation, and it does not preempt state trade secret law.[42] As recently as October 2011, Senators Herb Kohl and Christopher Coons

35. *Uniform Trade Secrets Act*, prefatory note, 14 U.L.A. 531 (2005) ("Notwithstanding the commercial importance of state trade secret law to interstate business, this law has not developed satisfactorily. In the first place, its development is uneven.").

36. MELVIN F. JAGER, TRADE SECRETS LAW §§ 2:3, 3:29 (2008); *see also supra* note 3.

37. Christopher Chantrill, *Comparison of State and Local Government Revenue and Debt in the United States Fiscal Year 2010*, USGOVERNMENTREVENUE.COM (Feb. 1, 2012), http://www.usgovernmentrevenue.com/state_rev_summary.php?chart=Z0&year=2010&units=d&rank=a.

38. For a complete list of states' enactments of and changes to the UTSA that is annually updated, *see* Brian M. Malsberger, TRADE SECRETS: A STATE-BY-STATE SURVEY (Brian Malsberger, Arnold H. Pedowitz & Robert A. Blackstone eds., 4th ed. 2011).

39. Michael Risch, *A Failure of Uniform Laws?*, 159 U. PA. L. REV. PENNUMBRA 1, 12 (2010), *available at* http://www.pennumbra.com/essays/10-2010/Risch.pdf.

40. *Hearing on H.R. 4651 Before the Subcomm. on Commerce & Fin. of the House Comm. on Interstate & Foreign Commerce*, 88th Cong., 2d Sess. 9 (1964). *See also* Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow The Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 505–08 (2010) (describing the Lindsay Bill).

41. Sandeen, *supra* note 40, at 509.

42. Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (2006).

introduced an amendment to the Economic Espionage Act that would provide a federal right of civil action for trade secret owners.[43] It's too early to tell how this most recent effort will fare. Today, though, there is still no general federal trade secret statute.

Commentators propose various theories to explain the sluggish development of trade secret law. According to one, trade secret owners have often been unaware that they have had a legally enforceable right; and even if they were aware of their rights, they were unwilling to pursue an action because doing so would require additional disclosures of the secret information.[44] Another commentator highlights the general unwillingness of courts to recognize new causes of action and the inability of Congress to agree on a definition of unfair competition, the general area of law into which trade secret law falls.[45] Others blame persistent legal questions, such as uncertainty about the precise parameters of trade secret protection,[46] including the nature of the property right and the definition of the public domain in the trade secret context.[47] Whatever the cause, the result is clear: trade secret law, compared to that of other types of IP, has been slow to take root.

III. SEVEN REASONS WHY TRADE SECRETS ARE INCREASINGLY IMPORTANT

Despite the relatively sluggish development of trade secret law, the influence of trade secrets is now expanding rapidly. Seven reasons help explain this phenomenon.

A. REASON NO. 1: NEW TECHNOLOGY

One reason for the ascendancy of trade secrets is that technology is making their misappropriation easier. Before computers, trade secret information was usually stored in physical form. Picture a locked file cabinet in a locked room in the basement of a secure manufacturing plant containing thousands of pages of blueprints for a new product. To steal those blueprints, a thief would have to gain access to the plant, to the room, and to the file cabinet. Then, the thief would have to either take the blueprints or

43. *See* Almeling, *supra* note 5.
44. Klitzke, *supra* note 34, at 284 n.37.
45. Sandeen, *supra* note 40, at 494, 507.
46. Klitzke, *supra* note 34, at 284 n.37.
47. *See* Charles Tait Graves, *Trade Secrets as Property: Theory and Consequences*, 15 J. INTELL. PROP. L. 39 (2007).

copy them, and loaded down with purloined documents, attempt to smuggle them out of the building.

Now picture the same blueprints in today's digital world. Depending on the sophistication of the trade secret owner, those blueprints would probably be stored as a digital file on a computer network. The file may be encrypted, password protected, and restricted to employees on a need-to-know basis. And the network might reside on a secure server behind a firewall. But if someone, such as a disgruntled employee, were to gain access to that file, she could easily download it, e-mail it, post it on the Internet, or simply save it on a flash drive and walk out the front door undetected, with thousands of pages of information in her pocket.[48] As noted by one commentator, "[t]he digital world is no friend to trade secrets."[49]

One recent example of such a disgruntled employee is Gary Min, who for ten years worked for E.I. du Pont de Nemours and Company, one of the world's preeminent chemical companies.[50] When DuPont demoted Min after he refused to relocate, Min decided to switch jobs. During his final months at DuPont, Min scoured his soon-to-be ex-employer's secure servers for information that would give his career at his new employer a head start.[51] He downloaded 22,000 abstracts and 16,700 documents—ten percent of the information stored on the confidential servers and fifteen times the number of documents accessed by the next most active user.[52] Most of these documents described DuPont's major product lines, such as Kevlar and Teflon, and bore no relation to Min's responsibilities at the company; the estimated value of the information was $400 million.[53] After the FBI learned of Min's actions and filed charges against him, Min pleaded guilty to theft of trade secrets and received eighteen months in prison.[54]

The risks to digital trade secret information are not confined to the risks posed by those with legitimate access. Hackers throughout the world can

48. *See* Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1, 2 (2007) (proposing a new test regarding the disclosure of trade secret information on the Internet).

49. Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA 359, 361 (2009).

50. Press Release, U.S. Dep't of Justice, Guilty Plea in Trade Secrets Case (Feb. 15, 2007), *available at* http://www.bis.doc.gov/news/2007/doj02_15_07.htm; *Jail Time Imposed in DuPont Spy Case*, NEWS JOURNAL, Nov. 7, 2007, at BA; Sean O'Sullivan, *Trade Case Reads like Spy Thriller*, NEWS JOURNAL, Feb. 16, 2007, at 1A.

51. *Id.*

52. *Id.*

53. *Id.*

54. *Jail Time Imposed in DuPont Spy Case*, NEWS J., Nov. 7, 2007, at BA; Sean O'Sullivan, *Trade Case Reads like Spy Thriller*, NEWS J., Feb. 16, 2007, at 1A.

break into networks and access confidential company information, including trade secrets, in ways that were unimaginable a few decades ago.[55] And the threat of hackers is rising. In 2002, for example, the F.B.I. handled nearly 1,500 hacking cases; in 2010, it handled more than 2,500.[56] One recent example is Philip Gabriel Pettersson, a.k.a. "Stakkato," who was indicted on five counts involving trade secret misappropriation.[57] He allegedly hacked into the ostensibly secure computer systems at Cisco Systems and NASA, including NASA's Advanced Supercomputing Division. Pettersson, a 16-year-old Swede, is accused of committing these acts from 5,000 miles away.

The risks posed by hackers are likely underreported because they are effective at covering their tracks. One recent study by Mandiant, a computer security firm, found that in cases handled by the firm where intrusions were traced to Chinese hackers, ninety-four percent of the targeted companies did not know of the breach until someone else told them.[58] And the median number of days between the intrusion and its detection was 416—more than a year.[59]

The risk to digital information continues to increase as more people acquire access to digital devices. In 2000, relatively few computers were connected to the Internet, but by 2010 there were more than ten billion computers with Internet access. Projections call for twenty-five billion of such devices by 2015, and by 2020, some fifty billion.[60]

Another trend that increases the risk of trade secret misappropriation is cloud computing—providing services and information over a network, typically the Internet, instead of keeping them within a company's secured proprietary network. Cloud computing is not new (think web-based e-mail like Hotmail, which launched in 1996), but what is new is that governments and businesses are increasingly storing sensitive and confidential data in the cloud.[61] While various providers of cloud services offer all sorts of

55. *See generally* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE 6–7 (2011) (citing a study from Cisco Systems) [hereinafter FOREIGN SPIES].

56. Devlin Barrett, *U.S. Outgunned in Hacker War*, WALL STREET J. (Mar. 28, 2012), http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html.

57. Press Release, U.S. Dep't of Justice, Kingdom of Sweden Accepts Request for Transfer of Prosecution in Case Involving Swedish National Charged with Hacking and Trade Secret Theft (Feb. 8, 2010), *available at* http://www.justice.gov/usao/can/press/2010/2010_02_08_sweden.transfer.press.html.

58. Barrett, *supra* note 56.

59. *Id.*

60. FOREIGN SPIES, *supra* note 55.

61. Horacio E. Gutiérrez, *Peering Through the Cloud: The Future of Intellectual Property and Computing*, 20 FED. CIR. B.J. 589, 589 (2011).

protections, moving data to the Internet increases the risk of that data being compromised. Questions about cloud computing—wondering, for example, how many years a client's cloud computing provider has been in business—are enough to keep a trade secret lawyer awake at night.

Just as the available methods to misappropriate trade secrets have proliferated, so too have the techniques for detecting such misappropriation. With today's technology, companies have access to a host of security systems: real-time computer monitoring technology; metadata about who accessed a file, when, for how long, and from where; the forensic ability to retrieve data that a misappropriator might delete in an effort to hide her tracks; video cameras; and key cards that track employee movements.[62] Buttressing these systems are network architecture and computer forensic technology, which go by names such as "deep packet inspection," "human behavior based network security," "insider threat tools," and many others.[63] Companies use these technologies to better detect who took what trade secret information and how.

B. REASON NO. 2: A CHANGING WORK ENVIRONMENT

As uncomfortable as it can be for companies to acknowledge, current and former employees are the groups most often sued for trade secret misappropriation.[64] Accordingly, an analysis of the growing importance of trade secrets should include consideration of changes in the American work environment.

One change is the increasing mobility of employees. No longer do workers think of themselves as "lifers," devoting their careers to a single employer. One government study found that a person born in the later years

62. IAN G. DIBERNARDO & JASON M. SOBEL, PROTECTING THE CONFIDENTIALITY AND VALUE OF SENSITIVE DATA AND INTELLECTUAL PROPERTY 2, 8 (2009) (instructing employees on the steps they can take to increase security of trade secrets, investigate breaches, and minimize the consequences of a breach).

63. MCAFEE, UNDERGROUND ECONOMIES: INTELLECTUAL CAPITAL AND SENSITIVE CORPORATE DATA NOW THE LATEST CYBERCRIME CURRENCY 17 (2011), *available at* http://www.mcafee.com/us/resources/reports/rp-underground-economies.pdf (defining "deep packet inspection" as software applications, lying on top of the hardware, that "allow for any kind of rules-based arrangement to strip data off packets leaving a network as well as prevent any type of exploit by stripping it from incoming traffic"; defining "human behavior based network security" as software that does "not use signatures, anomalies, or heuristics, but human behaviors that are common to all deceptive actions on a network which can be stopped prior to having data leave a network"; and defining "insider threat tools" as "tool [suites] that can be deployed on systems to monitor hundreds to thousands of inside users simultaneously, tracking their actions and identifying traits inherent in those actions that should be cause for alert").

64. *See Federal Study*, *supra* note 1, at 302–04; *State Study*, *supra* note 2, at 68–71.

of the Baby Boom, between 1957 and 1964, held an average of eleven jobs between ages eighteen and forty-two.[65] The greater the job mobility, the greater the opportunity to take and use a previous employer's trade secrets at a later position, whether accidentally or intentionally.

Another change that helps to explain the changing workforce is through sociological evidence. Professor Elizabeth Rowe recently published an article on the sociological aspects of trade secret misappropriation.[66] More than half of the current American workforce consists primarily of people from Generation X (born in the 1960s and 1970s) and Generation Y (born in the 1980s and early 1990s), and as Professor Rowe found, Gen X and Y workers generally don't feel that their jobs are secure.[67] Nor do they value loyalty to their current employers. They instead value mobility and entrepreneurism. The result is that these workers are more likely to move from job to job than generations past. And when they do, they are more likely to take their previous employers' trade secrets with them. The *Financial Times* recognized this trend in 2011 when it posed the question, "Is loyalty in the workplace dead?" and reported on the exacerbating trends of layoffs, outsourcing, and automation.[68] Another commentator notes that "shortening contracts, outsourcing, automation and multiple careers" may have given rise to the decrease in employee loyalty.[69]

Generation X is also the first group to have come of age around computers,[70] and Generation Y has never lived without them.[71] Both groups have a high comfort level with digital media and storage methods.[72] As explained above, advancing technology has increased opportunities for those

65. Press Release, Bureau of Labor Statistics of the U.S. Dep't of Labor, Number of Jobs Held, Labor Market Activity, and Earnings Growth Among the Youngest Baby Boomers: Results from a Longitudinal Survey 1 (Sept. 10, 2010), *available at* http://www.bls.gov/news.release/pdf/nlsoy.pdf (finding that "individuals born from 1957 to 1964 held an average of 11 jobs from age 18 to age 44").

66. *See* Elizabeth A. Rowe, *A Sociological Approach to Misappropriation*, 58 U. KAN. L. REV. 1 (2009) (suggesting that a sociological analysis of the values, characteristics, and employment expectations of so-called "New Generation Employees" helps explain current trends in trade secret law and should inform efforts to achieve optimal trade secret protection).

67. *Id.* at 6, 9.

68. *See* Phyllis Korkki, *The Shifting Definition of Worker Loyalty*, N.Y. TIMES, Apr. 23, 2011, at 1.

69. *Is Workplace Loyalty an Outmoded Concept?*, FIN. TIMES, Mar. 8, 2011, at 2 (quoting "the work expert," Lynda Gratton).

70. Rowe, *supra* note 66, at 6.

71. *Id.* at 9.

72. *Id.* at 6–7, 9–10.

with greater technical abilities to misappropriate trade secrets, often through the mere click of a mouse or the connection of a flash drive.

Another aspect of the modern work environment that may be contributing to the rise in trade secret litigation is the portability of work. As of 2011, 57 percent of employees save work to external devices on a weekly basis.[73] Another is the decreasing separation between work and home.[74] Employees can check their work e-mail from home or their personal e-mail from the office. Many employees work remotely from home at night and on weekends,[75] which creates more opportunities for leakage of trade secret information.

A final factor is the evolving perception of secrecy. IP law is based on the concept of ownership of information, and trade secret law in particular is based on owning confidential information. Generation Y and those even younger, however, came of age in a file-sharing culture where almost any information was free and easily available on the Internet. In 2000, for instance, Napster had approximately ten million users, mostly college students, sharing music in violation of copyright laws.[76] Those college students are now in the workforce, with access to their companies' trade secrets. Likewise, Facebook now has more than 800 million users,[77] many of whom post private, intimate information about themselves. In the short term, these changing social norms about protected information and privacy may help explain why trade secret misappropriation is increasing—why younger employees may think they are entitled to take certain information with them when they change jobs and why older employers may not agree.

In the long term, however, these norms actually may reduce the scope of trade secret protection. Norms change: America permitted drinking, then passed a constitutional amendment to forbid it, then passed another constitutional amendment to permit it.[78] If society embraces the "all information wants to be free" ethic, those norms may eventually undermine

73. FOREIGN SPIES, *supra* note 55, at A-3.

74. *See* Mickey Meece, *Who's the Boss, You or Your Gadget?*, N.Y. TIMES, Feb. 5, 2011, at BU1.

75. Lucy P. Eldridge & Sabrina Wulff Pabilonia, *Bringing Work Home: Implications for BLS Productivity Measures*, MONTHLY LAB. REV., Dec. 2010, at 18 (reporting that around eight percent of non-farm business employees do some work from home).

76. Matt Richtel, *Napster Has a New Interim Chief and Gets a $15 Million Investment*, N.Y. TIMES, May 23, 2000, at 1.

77. Nathan Olivarez-Giles, *Facebook F8: Redesigning and Hitting 800 Million Users*, L.A. TIMES (Sept. 22, 2011), http://latimesblogs.latimes.com/technology/2011/09/facebook-f8-media-features.html.

78. U.S. CONST. amend. XVIII, *repealed by* U.S. CONST. amend. XXI.

the policies that currently bolster robust trade secret protection. Companies and their lawyers should pay attention to these potential trends.

C. REASON NO. 3: INCREASING VALUE OF TRADE SECRET INFORMATION

Trade secrets matter more than ever because trade secrets, like all IP, are increasingly valuable and play an expanding role in the American economy. Describing IP generally, one team of economists concluded: "Extensive economic research and analysis have established that economically-powerful forms of intellectual property, embodied in innovations, are the largest single factor driving economic growth and development . . . ."[79]

The Congressional Research Service found this trend specifically applicable to trade secrets: "As the United States continues its shift to a knowledge- and service-based economy, the strength and competitiveness of domestic firms increasingly depends upon their know-how and intangible assets. Trade secrets are the form of intellectual property that protects this sort of confidential information."[80] Our current information-based economy represents a shift from the previous economy, which was based on physical assets such as natural resources and capital goods. Obvious examples of the nation's new direction are the dozens of modern industries that rely extensively on intellectual property for their value. These include the software industry, entertainment industries such as music and movies, Internet-based industries, and life science industries such as genetics, proteomics, and pharmaceuticals.

Statistics on trade secrets are hard to come by and even harder to rely upon. Still, those that exist do help in grasping the significance of trade secrets to companies. Consider the total value of the 500 companies, most of them publicly held, that constitute the S&P 500. Cornerstone Research has found that in 1975, 17 percent of the total value of the S&P 500 consisted of intangible assets, which encompasses trade secrets and other forms of IP; by 2009, the value had grown to 81 percent.[81] Similarly, Forrester Research estimates that trade secrets account for two-thirds of the value of most firms' information portfolios.[82]

---

79. Robert J. Shapiro & Kevin A. Hassett, *The Economic Value of Intellectual Property*, *in* USA FOR INNOVATION 20 (2005), *available at* http://www.sonecon.com/docs/studies/IntellectualPropertyReport-October2005.pdf.

80. JOHN R. THOMAS, CONG. RESEARCH SERV., R41391, THE ROLE OF TRADE SECRETS IN INNOVATION POLICY 2 (2010).

81. *See supra* note 8.

82. FORRESTER RESEARCH, INC., THE VALUE OF CORPORATE SECRETS: HOW COMPLIANCE AND COLLABORATION AFFECT ENTERPRISE PERCEPTIONS OF RISK 3 (2010).

As further evidence of the rising importance of trade secrets, consider the growing number of laws that criminalize trade secret misappropriation. In explaining why it passed the Economic Espionage Act, both the House and Senate Reports stated that Congress was reacting to the "growing importance of proprietary economic information," which, Congress prophesized, "will only continue to grow" as the "nation moves into the high-technology, information age."[83]

Washington is not only putting more emphasis on legal remedies for trade secret misappropriation, but also dedicating more resources to the enforcement of those laws. In 2010, the Department of Justice announced the Task Force on Intellectual Property and the appointment of fifteen new federal prosecutors and twenty new FBI agents to combat IP crime.[84] The steady stream of high-profile cases authorities have brought and settled is evidence of this dedication.[85] Among the feds' biggest catches of 2011 is Kexue Huang, who pleaded guilty to trade secret misappropriation from both Dow AgroSciences and Cargill.[86] Huang's first indictment in Indiana in 2010 was for misappropriation and transportation of Dow's trade secrets to China.[87] Later that year, a grand jury in Minnesota indicted Huang for trade secret misappropriation from Cargill.[88]

A final way to measure value is to analyze the cost of trade secret misappropriation. Estimates vary widely, but they often involve stratospheric

(defining "secrets" broadly to include "information that the enterprise creates and wishes to keep under wraps").

83. H.R. REP. NO. 104-788, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023–25; S. REP. NO. 104-359, at 7–8 (1996).

84. Jonathan B. New & Christy Nixon, *DOJ Steps up Prosecution for Trade Secret Theft*, NAT'L L. J., Jan. 31, 2011, at 14 (stating that, in 2010, the FBI opened at least sixty-six new crime investigations involving the alleged misappropriation of trade secrets).

85. 2010 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT 59–60 (2011).

86. Andrew Harris, *Ex-Dow Scientist Admits to Economic Espionage, U.S. Says*, BLOOMBERG (Oct. 18, 2011), http://www.businessweek.com/news/2011-10-18/ex-dow-scientist-admits-to-economic-espionage-u-s-says.html. The two cases were consolidated in the District Court for the Southern District of Indiana. United States v. Huang, Nos. 1:10-CR-00102 & 1:11-CR-00163 (S.D. Ind. 2010); Press Release, U.S. Department of Justice, Chinese National Pleads Guilty to Economic Espionage and Theft of Trade Secrets (Oct. 18, 2011), *available at* http://www.justice.gov/opa/pr/2011/October/11-crm-1372.html [hereinafter Chinese National Press Release].

87. Chinese National Press Release, *supra* note 86. Huang's disclosure of Dow's trade secrets to Hunan University in China also resulted in an indictment for foreign transportation of stolen property. *Plea Agreement Reached in Trade Secret Theft Case*, BLOOMBERG BUSINESSWEEK, Sept. 15, 2011, http://www.businessweek.com/ap/financialnews/D9PP88N00.htm.

88. Harris, *supra* note 86.

numbers. ASIS International, a professional association of security managers, placed the cost of trade secret misappropriation in the United States in 2006 at $300 billion.[89] Using different metrics, McAfee, the computer security giant, estimated that in 2008 data leaks cost companies around the globe more than $1 trillion.[90]

D. REASON NO. 4: THE UTSA

Another reason for the rise in trade secrets generally, and trade secret litigation in particular, is the growth of a well-developed body of trade secret law. As of today, forty-seven states and the District of Columbia have enacted the UTSA in some form.[91]

To be clear, the UTSA itself has not caused the growth in trade secret litigation. While trade secret litigation has increased in the states that have enacted the UTSA, the three states that did not (Massachusetts, New York, and Texas) have seen increased trade secret litigation as well.

The point is that the widespread adoption of the UTSA has increased awareness of trade secret law—among lawyers, companies, judges, and others—and has provided greater consistency in the application of trade secret law and in the laws themselves. Before the UTSA, the states had greater disparities among themselves on various trade secret issues, ranging from the types of conduct that constituted trade secret misappropriation to the remedies afforded. The UTSA is not perfect, and trade secret law still varies from state to state in frustrating ways.[92] But the UTSA has provided a necessary starting point, establishing a template for legal remedies to trade secret misappropriation.[93]

---

89. ASIS INTERNATIONAL, TRENDS IN PROPRIETARY INFORMATION LOSS 10 (2007), *available at* http://www.asisonline.org/newsroom/surveys/spi2.pdf.

90. Press Release, McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property (Jan. 29, 2009), *available at* http://www.businesswire.com/news/home/20090129005493/en/McAffee-Research-Shows-Global-Recession-Increasing-Risks.html.

91. 1 MELVIN F. JAGER, TRADE SECRETS LAW § 3:29 (2011) (providing citations to statutes in the District of Columbia and the states that have enacted the UTSA).

92. David S. Almeling, *A Practical Case For Federalizing Trade Secret Law*, LAW360 (June 23, 2009), http://www.law360.com/articles/106724 (identifying six examples of interstate variations in trade secret law, presenting the practical problems these variations cause, and proposing federalization of trade secret law); *see also* Michael H. Bunis & Anita Spieth, *Common Law v. UTSA: The Last States Standing*, LAW 360, Apr. 2, 2012, http://www.law360.com/ip/articles/321776?nl_pk=86604097-1f36-4bfa-a7ca-96c7182cf1bc&utm_source=newsletter&utm_medium=email&utm_campaign=ip (identifying "dissimilarities in the trade secret jurisprudence among different states").

93. Risch, *supra* note 39, at 1 (stating that "[u]niform laws like the UTSA" provide "a consistent set of rules to provide settled expectations for interstate activities").

Thus, it is increasingly true that if a company protects its valuable information as trade secrets, there is a large, growing, well-developed, and relatively consistent body of law on which that company can rely to protect the information. The growth of trade secret litigation may have, indeed, created a positive feedback loop: more companies rely on trade secrets, which causes plaintiffs to bring more trade secret cases to the courts, which causes the body of trade secret law to develop further, which provides the doctrinal stability needed for more companies to rely on trade secrets. Please forgive the tautology, but the growth in trade secret litigation appears to be fueling a growth in trade secret litigation.

E. REASON NO. 5: FLEXIBLE (AND EXPANDING) SCOPE OF TRADE SECRETS

Another cause of the increase in trade secret litigation is the flexible definition of trade secrets. Because a "trade secret" is broadly defined as *any* information that is secret, derives economic value from that secrecy, and is the subject of reasonable measures to maintain its secrecy,[94] the category of material falling within this definition is continually expanding.

A small sample of the types of trade secrets that have been recognized by the courts includes chemical formulas, source code, methods, prototypes, prerelease pricing, financials, budgets, contract terms, business plans, market analyses, salaries, information about suppliers and customers, experiments, positive and negative experimental results, engineering specifications, laboratory notebooks, and recipes.[95] Real-world examples of this breadth encompass subject matter ranging from Church of Scientology religious texts[96] to a concept for a clickety-clacking railroad toy[97] to standardized tests for ninth graders.[98] The definition of a trade secret is potentially so broad that the meaning of "trade secret" is often defined by what it is not. Courts use the concept of an employee's "tool kit," or her generalized skills, knowledge, training, and experience,[99] to cabin the scope of trade secret law.

---

94. Uniform Trade Secrets Act (amended 1985), 14 U.L.A. 529, § 1(4) (2005).

95. MICHAEL A. EPSTEIN, EPSTEIN ON INTELLECTUAL PROPERTY § 1.02[E][1] (5th ed. 2008 & Supp. 2009) ("As long as the definitional elements are met, virtually any subject matter or information can be a trade secret.").

96. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231 (N.D. Cal. 1995).

97. Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714 (7th Cir. 2003).

98. Prosonic Corp. v. Stafford, 539 F. Supp. 2d 999 (S.D. Ohio 2008).

99. JAMES POOLEY, TRADE SECRETS § 4.01[3][b] (2010) (describing the concept of an employee's personal "tool kit").

While the definition of a trade secret has long been broad, this breadth may end up contributing to a continued rise in trade secret litigation because it means that trade secret law is perfectly suited to the evolutionary (progression of old ideas) and revolutionary (creation of new ideas) nature of innovation.[100] As noted by one prominent commentator, "[T]rade secrets have gained importance because in many fields, the technology is changing so rapidly that it is outstripping the existing laws intended to encourage and protect inventions and innovations."[101]

One interesting, complicating issue regarding the definition of trade secretsis how technology may change the scope of trade secret protection in varying ways. Consider a recent case involving the interplay between a trade secret customer list and search engine technology. In 2010, recruiting company Sasqua Group sued its former employee for trade secret misappropriation of its customer information database.[102] The court acknowledged that the information in Sasqua's database "may well have been a protectable trade secret in the early years of Sasqua's existence when greater time, energy and resources may have been necessary to acquire the level of detailed information to build and retain the business relationships at issue here."[103] At the time of litigation, however, the court stated that the "exponential proliferation of information" on the Internet, including search engines and social media, makes this "a very different story," especially because the defendant demonstrated that the alleged trade secrets (i.e., information about customers) were readily available on the Internet.[104] The customer list is perhaps the quintessential trade secret, and one of the types of trade secrets that parties litigate most often.[105] The *Sasqua* court did nothing to change that, as the court recognized that the law certainly permits trade secret protection for some customer databases in the Information Age.

---

100. For one example of the flexible use of trade secret law to address thorny subject matter, *see generally* Deepa Varadarajan, *A Trade Secret Approach to Protecting Traditional Knowledge*, 36 YALE J. INT'L L. 371, 417 (2011) (addressing the difficult subject matter issue of traditional knowledge within various intellectual property regimes and arguing that "[t]rade secret law can be a useful legal vehicle for traditional knowledge holders when dealing with outsiders' improper acquisition, disclosure, and use of relatively secret information").

101. JAGER, *supra* note 36, at § 1:1. An experienced patent litigant might respond that patent law also encompasses "anything under the sun that is made by man." Diamond v. Chakrabarty, 447 U.S. 303, 309 (1980). While this is true, in practice the scope of patent law is narrower than that of trade secret law.

102. Sasqua Gr., Inc. v. Courtney, No. CV-10-528, 2010 WL 3613855, at *3 (E.D.N.Y. Aug. 2, 2010) (report and recommendation adopted Sept. 7, 2010).

103. *Id.* at *22.

104. *Id.*

105. *State Study*, *supra* note 2, at 72.

The court merely decided that Sasqua's database was not one of them. In short, while trade secrets encompass a broad range of subject matter that expands to accompany new technologies, some new technologies and trends—such an Internet search sites and the placement of once-private information online through social media—cause the scope of trade secret law to shrink.[106]

F. REASON NO. 6: THE RISE OF INTERNATIONAL THREATS

While U.S. citizens and companies steal trade secrets, increased threats from foreign individuals, companies, and governments also contribute to the growing importance of trade secrets.

By enacting the Economic Espionage Act in 1996, Congress sought in part to address the rise of trade secret misappropriation from foreign entities.[107] That is why one of the Act's two main provisions criminalizes misappropriating trade secrets with the knowledge or intent that the misappropriation will benefit a "foreign power."[108] President Obama has also stressed the threat of foreign economic espionage, warning in 2011 that "[t]he pace of foreign economic collection and industrial espionage activities against major U.S. corporations and U.S. [g]overnment agencies is accelerating."[109] And Robert S. Mueller III, the director of the F.B.I., reiterated those concerns when he stated that cyberattacks would soon replace terrorism as the agency's primary concern as hackers, particularly from China, steal huge amounts of valuable data and intellectual property from American companies.[110]

Several factors explain the rise in international threats. One is the internationalization of business. More and more U.S. companies operate internationally, whether tapping supply chains that employ foreign

106. While new technologies may expose certain once-protected information and thus render that information ineligible for trade secret protection, information disclosed through social media could still be protected. *See, e.g.*, Christou v. Beatport, L.L.C., No. 10-cv-02912, 2012 WL 872574, at *17 (D. Colo. Mar. 14, 2012) (denying a motion to dismiss, reasoning that "[w]hether plaintiffs' MySpace friends list is a trade secret is question of fact"); PhoneDog v. Kravitz, No. 11-03474, 2011 WL 5415612 (N.D. Cal. Nov. 11, 2011) (denying a motion to dismiss that argued that the identity of Twitter followers and the password to their Twitter accounts could not constitute trade secrets).

107. *See generally* H.R. REP. NO. 104-788 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023–25 ("More disturbingly, there is considerable evidence that foreign governments are using their espionage capabilities against American companies."); S. REP. NO. 104-359, at 7 (1996).

108. 18 U.S.C. § 1831 (1996).

109. FOREIGN SPIES, *supra* note 55, at iii.

110. Richard A. Clarke, *How China Steals Our Secrets*, N.Y. TIMES, Apr. 2, 2012, http://www.nytimes.com/2012/04/03/opinion/how-china-steals-our-secrets.html?_r=1.

manufacturers or relying on foreign capital markets. Simply put, as more American companies venture overseas and take their trade secrets with them, those trade secrets become more vulnerable to misappropriation by foreign parties.

Another factor is technology. As detailed above, hackers can access trade secrets from anywhere in the world. No longer do thieves need to physically abscond with the trade secrets. All they need is a computer with an Internet connection.

Further, certain countries view stealing trade secrets as an aid to development. As summarized by President Obama, "Chinese leaders consider the first two decades of the 21st century to be a window of strategic opportunity for their country to focus on economic growth, independent innovation, scientific and technical advancement, and growth of the renewable energy sector," and "China's intelligence services, as well as private companies and other entities, frequently seek to exploit Chinese citizens or persons with family ties to China who can use their insider access to corporate networks to steal trade secrets using removable media devices or e-mail."[111] Of the seven Department of Justice prosecutions under the Economic Espionage Act in 2010, six involved a link to China.[112]

One recent example of trade secret theft involving China is the case of Xiang Dong "Mike" Yu, a project engineer for the Ford Motor Company who smuggled Ford trade secrets to China while on a job hunt that led to a position with one of Ford's competitors, Foxconn PCE Industry, Inc.[113] Yu copied 4,000 Ford documents, estimated to be worth between $50 million and $100 million, onto an external hard drive and delivered them to a Foxconn manager at that manager's residence in Shenzhen. The documents contained trade secret design specifications for engines and electric power supply systems. The United States government launched an aggressive prosecution under the federal Economic Espionage Act, seeking, in the words of the U.S. Attorney in Detroit, Barbara L. McQuade, to "protect the intellectual property of our U.S. automakers, who invest millions of dollars and decades of time in research and development to compete in a global

111. *Id.* at 5.

112. *Id.*

113. *See* Erin Marie Daly, *Ex-Ford Worker Gets 6 Years for Trade Secrets Theft*, LAW360.COM (April 12, 2011), http://www.law360.com/topnews/articles/210020/ex-ford-worker-gets-6-years-for-trade-secrets-theft; Ben Klayman, *Ex-Ford Engineer Sentenced for Trade Secrets Theft*, REUTERS.COM (April 13, 2011), http://www.reuters.com/article/2011/04/13/us-djc-ford-tradesecrets-idUSTRE73C3FG20110413.

economy."[114] Yu pleaded guilty, and in 2011, a federal judge sentenced him to nearly six years in prison followed by deportation to China.

Although China may be widely perceived as the largest international threat to trade secret misappropriation, it is not the only one. Surveys in 2008 and 2010 found that more than one thousand information technology professionals perceive that Pakistan, Russia, and India loom right behind.[115]

A major issue with the rise of international trade secret misappropriation is the difficulty in enforcement. Depending on the facts of the misappropriation, U.S. courts may not have jurisdiction to hear the case.[116] Obtaining justice in foreign countries is likewise difficult because foreign countries vary widely in their judicial procedures, trade secret protection, and respect for the rule of law. International treaties help protect trade secrets, principally Article 1711 of the North American Free Trade Agreement[117] and Article 39 of the Trade-Related Aspects of Intellectual Property Rights.[118] But not all countries adhere to these rules, and even in some countries that do, cultural norms and enforcement problems can weaken trade secret protection. Although China, for example, has rules that protect trade secret rights, enforcement is complicated and expensive, and there is a high burden of proof that makes litigation an ineffective way to protect trade secrets in all but the clearest cases.[119] The European Union, for another example, has a

114. DOJ press release, *Chinese National Sentenced Today For Stealing Ford Trade Secrets* (Apr. 12, 2011), *available at* http://www.justice.gov/usao/mie/news/2011/2011_4_12_xyu.html.

115. MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 1, 12 (2009) ("Three countries, in particular, stood out to the survey respondents—perhaps reflecting broader security perceptions. Respondents cited China, Pakistan and Russia as the worst-rated countries when it comes to the protection of digital assets. Pakistan, China and Russia, in that order, were also perceived to have the worst reputations for pursuing or investigating security incidents."); MCAFEE, UNDERGROUND ECONOMIES: INTELLECTUAL CAPITAL AND SENSITIVE CORPORATE DATA NOW THE LATEST CYBERCRIME CURRENCY 10 (2011) (presenting data of countries with which companies have avoided doing business).

116. *See* TianRui Group Co. Ltd. v. Int'l Trade Comm'n, 661 F.3d 1322 (Fed. Cir. 2011) (finding that, on the facts of this particular case, the U.S. International Trade Commission had jurisdiction to address trade secret misappropriation that occurs in a foreign country, but in other situations, the presumption against extraterritoriality would govern).

117. North American Free Trade Agreement, art. 1711, U.S.-Can.-Mex., Dec. 17, 1992, 32 I.L.M. 605 (1993).

118. Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Counterfeit Goods, art. 39, Dec. 15, 1993, 33 I.L.M. 81 (1994).

119. J. Benjamin Bai & Guoping Da, *Strategies for Trade Secrets Protection in China*, 9 NW. J. TECH. & INTELL. PROP. 351, 366 (2011) (demonstrating that while a higher burden of proof and the absence of a U.S.-style discovery procedure make it difficult to enforce trade secret laws in Chinese courts, companies have nevertheless succeeded by following certain practices. Such strategies include requesting evidence preservation orders in civil cases,

patchwork of laws that do not always protect the trade secret owner. As a 2012 publication of the European Commission described, "[i]n some countries the protection is effective; in others—sometimes because of the difficulty in enforcement—the law provides inadequate protection" for trade secrets.[120]

G. REASON NO. 7: INTERACTION WITH PATENT LAW

Recent U.S. patent law developments have tilted the balance between whether a business should pursue patents or trade secrets.

Talk of trade secrets often brings up talk of patents because they both protect some of the same types of information. The owner of certain kinds of information—including formulas, computer programs, and manufacturing processes—may have the option of pursuing either trade secret or patent protection. But the subject matter of patents and trade secrets is far from coextensive. While any information can be a trade secret, for example, patents cover a much narrower range of subject matter. Also, many categories of trade secrets—among them customer lists, financial information, HR data, and business strategy—are not eligible for patent protection.

The reason to discuss patents in an article about the growth of trade secret litigation is that in situations that present a company the option of patent or trade secret protection, the critical question is which to pursue. There is no simple answer.[121]

While companies continue to protect certain types of information as patents (patent litigation increased about 300 percent from 1990–2004, and has been roughly steady since),[122] there are several recent trends that affect a company's choice and may contribute to an increased reliance on trade secrets.

---

utilizing the criminal court system, and actively employing preventative measures, such as confidentiality and non-compete agreements).

120. HOGAN LOVELLS INT'L LLP, REPORT ON TRADE SECRETS FOR THE EUROPEAN COMMISSION 43 (2012), *available at* http://ec.europa.eu/internal_market/iprenforcement/docs/trade/Study_Trade_Secrets_en.pdf.

121. *See, e.g.*, Atl. Research Mktg. Sys., Inc. v. Troy, 659 F.3d 1345, 1357 (Fed. Cir. 2011) (recognizing "the inherent tension" created by alleging that a defendant "misappropriated trade secrets, while simultaneously asserting that the products [the defendant] Troy developed with the misappropriated trade secrets infringed [the plaintiff's] patent).

122. Kyle Jensen, *Guest Post: Counting Defendants in Patent Litigation*, PATENTLY-O (Oct. 27, 2010), www.patenlyo.com/patent/2010/10/guest-post-counting-defendants-in-patent-litigation.html.

In 2011, having debated a patent bill each of the previous six years, Congress finally passed the Leahy-Smith America Invents Act ("AIA"), the largest legislative reform of patent law since the U.S. Patent Act of 1952.[123] The AIA makes dozens of changes to patent law, some of which reduce the incentive to patent inventions and also to assert those patents in litigation—reforms that increase the incentive to rely on trade secret protection. For example, the AIA expands the prior-use defense, meaning that companies that would otherwise infringe a patent have a defense if they were engaging in those acts prior to the patent's filing;[124] because such use often is confidential and maintained as a trade secret, this provision benefits trade secret owners. But many practitioners, including the author, believe that the prior use defense does not dramatically reconfigure the balance between patents and trade secrets.[125] The AIA also raises the standard for which defendants can be joined in the same action,[126] which removes a litigation strategy used by many patent plaintiffs to force companies, sometimes competitors, to have to litigate in the same action. Furthermore, the AIA lowers the standards for *inter partes* reexamination from "substantial new question of patentability" to "a reasonable likelihood that the requestor will prevail"[127] and enables third parties to submit information that may be relevant to the granting of a patent.[128]

But the AIA is not a lopsided win for defendants, and it contains some provisions that make patents more desirable, including permitting patent owners to cure inequitable conduct and reducing the threat of false marking litigation.[129] The AIA also benefits patent owners by providing more money to the U.S. Patent & Trademark Office, which has been increasingly slow to issue patents: in 1997 there were 2.25 patents pending for every one issued, but by 2008 the rate had risen to 6.6 pending patents to every issued

123. *See* Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (codified as amended in scattered sections of 35 U.S.C.).

124. *Id.* § 5(a) & (c). For a detailed description of the defense written by the U.S. Patent & Trademark Office, *see generally* U.S. PATENT & TRADEMARK OFFICE, REPORT TO CONGRESS ON THE PRIOR USER RIGHTS DEFENSE (2012).

125. David S. Almeling & Darin W. Snyder, *Guest Post: The New, Improved Prior Use Defense: The Same Patent vs. Trade Secret Calculus*, TRADE SECRET LITIGATOR (Apr. 17, 2012), http://www.hahnloeser.com/tradesecretlitigator/post/2012/04/17/Guest-Post-David-Almeling-and-Darin-Snyders-Take-on-the-Prior-Use-Defense-under-the-America-Invents-Act-and-Trade-Secrets-No-Big-Deal!.aspx.

126. *Id.* § 19(d)(1).

127. *Id.* § 6(c)(3)(A)–(B).

128. *Id.* § 8.

129. *See id.* § 16(a)–(b).

patent.[130] The AIA thus cuts both ways, but in the end, it does more to restrict the power of patent owners and plaintiffs, potentially causing more companies to prefer trade secret protection for certain inventions.

In addition to the AIA, a series of recent Supreme Court decisions tilts the patent-vs.-trade-secret calculus in favor of trade secrets.[131]

In its 2012 decision in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, the Supreme Court applied the law-of-nature exception, reversing the Federal Circuit and invalidating a patent that claimed a method for determining dosing ranges of drugs used to treat autoimmune diseases.[132] The Court focused on the intersection between patents that claim non-patentable "laws of nature, natural phenomena, and abstract ideas" and those that claim a patent-eligible "application of a law of nature or mathematical formula to a known structure or process."[133] This decision, which arguably expands the law-of-nature exception, especially in the pharmacology and biotechnology industries, could cause life science and other companies to reconsider whether to pursue patent or trade secret protection. If they decide to pursue patent protection, the decision could impair the scope and even validity of the resulting patents.

In *Bilski v. Kappos*, the Supreme Court in 2010 revised what should be the appropriate test for patentable subject-matter eligibility and narrowed protections for business method patents, holding that the claims at issue (involving a hedging method for commodities) were not patentable processes because they are attempts to patent abstract ideas.[134]

In *KSR International Co. v. Teleflex, Inc.*, the Supreme Court in 2007 revisited the nonobviousness standard for the first time in forty years.[135] The Court reversed a lower court's decision that a particular patent would not have been obvious and limited which inventions are sufficiently nonobvious to qualify for patent protection. *KSR* thus increased the burden of obtaining

130. *Patent Office — "First to File" Bill (2011)*, N.Y. TIMES, Sept. 9, 2011, http://topics.nytimes.com/top/news/science/topics/inventions_and_patents/index.html.

131. R. Mark Halligan, *Trade Secrets v. Patents: The New Calculus*, ABA Intellectual Property Law (ABA-IPL) LANDSLIDE 10, 10–13 (July/Aug. 2010) (summarizing some of these decisions), *available at* www.americanbar.org/content/dam/aba/migrated/intelprop/magazine/LandslideJuly 2010_halligan.authcheckdam.pdf.

132. 132 S. Ct. 1289, 1294 (2012).

133. *Id.* at 1293–94.

134. Bilski v. Kappos, 130 S. Ct. 3218, 3329–30 (2010); *see generally* Dennis Crouch & Robert P. Merges, *Operating Efficiently Post-Bilski by Ordering Patent Doctrine Decision-Making*, 25 BERKELEY TECH L.J. 1673 (2010) (describing ways to minimize the cost of administering the holding in *Bilski*).

135. 550 U.S. 398 (2007).

and enforcing a patent. In obtaining a patent, *KSR* means that the patent office is more likely to find that an alleged invention is obvious and thus not entitled to patent protection.[136] Finally, in litigation, *KSR* means that alleged infringers have a greater ability to argue that an issued patent is obvious and should not have been issued at all.[137]

In *eBay Inc. v. MercExchange, L.L.C.*, the U.S. Supreme Court in 2006 raised the threshold for obtaining an injunction.[138] In rejecting the then-prevailing rule that an injunction may issue automatically on a finding of patent infringement, the Court held that a federal court must still weigh the four factors traditionally used to determine if an injunction should issue: "(1) that [the plaintiff] has suffered an irreparable injury; (2) that remedies available at law . . . are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction."[139] With this decision, the Court reduced the threat of an injunction from a patent infringement case and, therefore, decreased the potential reward in asserting patent infringement and the concomitant risk in defending against that assertion.

Finally, in a series of recent cases, including *Uniloc USA, Inc. v. Microsoft Corp.*,[140] *ResQNet.com, Inc. v. Lansa, Inc.*,[141] and *Lucent Technologies, Inc. v. Gateway, Inc.*,[142] the Federal Circuit has gradually reduced the amount of compensatory and enhanced damages for patent infringement.

Another change in patent law that affects trade secret law is the eighteen-month publication rule of the American Inventors Protection Act of 1999. Before 1999, applicants were in a win-win situation. They could file a patent application for their trade secret and be assured that they would either obtain a patent (if the patent issued) or retain their trade secret (if the application was denied). Under the eighteen-month publication rule, however, a regular U.S. patent application will be published eighteen months after filing unless

136. JANICE M. MUELLER, PATENT LAW 219 (3d ed. 2009).

137. *Id.* at 219–24.

138. 547 U.S. 388 (2006).

139. *Id.* at 391–92.

140. 632 F.3d 1292 (Fed. Cir. 2011) (overturning a $388 million jury verdict and holding that the "25 percent rule" is a "fundamentally flawed tool for determining a baseline royalty rate in a hypothetical negotiation").

141. 594 F.3d 860 (Fed. Cir. 2010) (vacating a $500,000 damages award based on a 12.5% royalty rate and reasoning that the royalty rate was excessive and inadequately supported by the evidence).

142. 580 F.3d 1301 (Fed. Cir. 2009) (vacating the jury's $358 million damages award and reasoning that the damages award was not supported by the evidence).

certain steps are taken.[143] Applicants have to gamble because if they file a patent application that does not mature into an issued patent, they have neither trade secret nor patent protection. Few applicants take these protective steps: 85 percent of applications filed by large entities, and 74 percent of those filed by small entities, were published under this rule.[144] It thus appears that some applicants are not taking this risk and, instead, are forgoing patent protection for trade secret protection.

Cost is another consideration that weighs in favor of trade secrets. Patents are increasingly expensive to obtain, maintain, and enforce, including the cost of obtaining patent rights in each country.[145] In contrast, there are no formal requirements to designate information as trade secrets, since they exist without any specific filing procedure. And while a trade secret owner must take reasonable steps to ensure secrecy, courts generally have held that reasonableness is a relatively lax standard.[146] Patents, on the other hand, require the monitoring and payment of maintenance fees that, if missed, can result in the loss of rights.[147] Another major cost differential between the two categories is litigation. For high-stakes litigation, defined as litigation in which more than $25 million is at risk, the reported average cost to handle patent litigation in 2009 was $5.5 million while the cost for trade secret litigation was $2.2 million.[148] Trade secret litigation has long cost less; in 2001, patent litigation ran $3 million compared with $1 million for trade secret litigation.[149]

None of this is to say that companies should always choose trade secret protection over patents. Indeed, patents are better at protecting certain types of inventions and for implementing certain types of business strategies. The point here is that given the partial overlap between patent and trade secret protection, the changing scope of patent law might encourage a company to use trade secret law instead. Indeed, new survey findings from the National Science Foundation and the U.S. Census Bureau suggest this trend. While the numbers differ across industries, most businesses identified trademarks and

143. 35 U.S.C. § 122(b)(1)(A) (2006).

144. U.S. GOV'T ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL COMMITTEES: PATENTS: INFORMATION ABOUT THE PUBLICATION PROVISIONS OF THE AMERICAN INVENTORS PROTECTION ACT 4 (2004).

145. GURIQBAL SINGH JAIYA & CHRISTOPHER M. KALANJE, MANAGING PATENT COSTS: AN OVERVIEW 10–11 (2006), *available at* http://www.wipo.int/export/sites/www/sme/en/documents/pdf/managing_patent_costs.pdf.

146. Reasonable measures need not be perfect or heroic; they only need to be reasonable. POOLEY, *supra* note 99, at § 4.04[2][b] ("No system is perfect, and the people who put it to use certainly are not perfect. Some mistakes are permitted.").

147. 35 U.S.C. § 41(b) (2006).

148. AM. INTELL. PROP. LAW ASS'N, REPORT OF ECONOMIC SURVEY 29–30 (2009).

149. AM. INTELL. PROP. LAW ASS'N, REPORT OF ECONOMIC SURVEY 25–26 (2007).

trade secrets as important forms of IP protection, followed by copyrights, and then by patents.[150]

IV. CONCLUSION (AND A PREDICTION)

Understanding trade secrets requires more than knowledge of the law. It is also about the evolving technologies, social norms, politics, economics, and other factors that shape the use and misuse of trade secrets. This Article presented seven such factors that help explain the increasing importance of trade secrets.

Identifying causes for the remarkable growth of trade secrets over the past few decades does not, however, foretell whether these trends will continue. Some of the seven factors discussed above, in fact, augur neither more nor less trade secret litigation. The balance between patent law and trade secret law, for example, has varied over the past few decades as Congress and courts intermittently bolstered or hampered the patenting of inventions.

Still, most of the factors discussed above show no sign of abating. It is difficult to imagine technology, for example, regressing to a world of hard-copy documents and file cabinets. The shift from an economy based on capital goods toward one based on informational assets has been a constant over the past half-century and appears to be continuing in that direction. Courts' familiarity and comfort with the UTSA will only increase as companies file more trade secret cases and courts hear those cases. And the relentless internationalization of business will continue to expose American companies' trade secrets to misappropriation by foreign entities.

In short, the seven trends discussed here, and the corresponding boom in trade secret litigation, suggest that trade secrets will only become more important in years to come.

150. JOHN E. JANKOWSKI, BUSINESS USE OF INTELLECTUAL PROPERTY PROTECTION DOCUMENTED IN NSF STUDY, INFOBRIEF 1 (Feb. 2012), *available at* http://www.nsf.gov/statistics/infbrief/nsf12307.