KILLING THE GOLDEN GOOSE: THE DANGERS OF STRENGTHENING DOMESTIC TRADE SECRET RIGHTS IN RESPONSE TO CYBER-MISAPPROPRIATION

Zoe Argento*

16 YALE J.L. & TECH. 172 (2014)

ABSTRACT

Hackers all over the world exploit our reliance on computer systems to take American trade secrets. The response will likely be a dramatic strengthening of trade secret law. Congress has already passed statutes strengthening trade secret law, and more bills are pending. The alarmist rhetoric on cyber-risks to trade secrets, however, ignores the most dangerous risk. By over-reacting to the threat of cyber-misappropriation, we may suppress the innovation and competition that produce our trade secrets in the first place. This paper uses an array of studies on cyber-risks and trade secret litigation to show that bolstering trade secret rights will have little effect on cyber-misappropriation. The evidence indicates that trade secret holders cannot and will not pursue cyber-misappropriators in court for technological and business reasons, not for legal reasons. Worse, strengthening trade secret law will cause significant collateral damage. Trade secret holders will use stronger trade secret rights in other types of misappropriation cases to impede follow-on innovation, restrict worker mobility, dampen competition, and hamper public access to useful information. In short, the costs outweigh the benefits of bolstering trade secret law to combat cyber-misappropriation of trade secrets.

* Associate Professor, Roger Williams University School of Law. The author would like to thank Sharon Sandeen and David Levine for their comments and Mackenzie Flynn and Ryan McCaffrey for their research assistance. Mistakes, if any, are the sole responsibility of the author.

In one of Aesop's fables, a farmer had a goose that laid golden eggs. Hoping to discover the source of the gold, he killed the goose. The farmer found nothing, and that, of course, was the end of the golden eggs.

In 21st century America, a different form of golden eggs is under threat—immensely valuable trade secrets encompassing much of the innovation and business strategy that power our economy. Cyber-hackers all over the world have dedicated their efforts to breaching American companies, research institutions, and government agencies to take them. Many of these hackers are well-organized and well-financed. Some are even state-sponsored. In January 2013, for example, the security firm Mandiant reported that a unit of the Chinese army had breached 115 American companies, sometimes retaining clandestine access over the course of

years.[1] The problem of cyber-intrusion is pervasive and growing. For example, in one survey in 2011, companies reported an average of 1.4 successful attacks per week, a 44 percent increase from the previous year.[2]

Our worries over losing trade secrets to cyber-intruders, however, may lead us to kill our own golden goose—the vigorous competition and culture of innovation that produce our trade secrets.

One of our greatest strengths as a nation is our innovative and entrepreneurial culture. Our country produced the airplane, the assembly line, the laser, the personal computer, the internet . . . the list goes on and on.[3] Innovation is a key driver of U.S. economic growth and national competitiveness.[4]

The success of American innovation stems from many factors—capital markets, an educated populace, infrastructure, funding for basic research, among others—but one important factor is our system of intellectual property law, particularly trade secret law.[5]

---

[1] MANDIANT, APT 1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 21 (Jan. 2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [hereinafter MANDIANT APT 1].

[2] PONEMON INSTITUTE, SECOND ANNUAL COST OF CYBER CRIME STUDY: BENCHMARK STUDY OF U.S. COMPANIES 2 (Aug. 2011), *available at* http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf [hereinafter PONEMON STUDY].

[3] JAMES WEI, GREAT INVENTIONS THAT CHANGED THE WORLD 218 (airplane), 278 (internet) (Wiley 2012); DAVID E. NYE, AMERICA'S ASSEMBLY LINE 36 (MIT Press 2013), *available at* http://mitpress.mit.edu/books/americas-assembly-line (assembly line); American Institute of Physics, *Bright Ideas: The First Lasers*, http://www.aip.org/history/exhibits/laser/sections/whoinvented.html (lasers).

[4] CHARLES SCHULTZE, MEMOS TO THE PRESIDENT: A GUIDE THROUGH MACROECONOMICS FOR THE BUSY POLICYMAKER 299 (1991); ECONOMICS AND STATISTICS ADMINISTRATION AND THE UNITED STATES PATENT AND TRADEMARK OFFICE, INTELLECTUAL PROPERTY AND THE U.S. ECONOMY: INDUSTRIES IN FOCUS v (March 2012), *available at* http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf.

[5] U.S. DEP'T OF COMM., THE COMPETITIVENESS AND INNOVATIVE CAPACITY OF THE UNITED STATES 2-1 (Jan. 2012), *available at* http://www.commerce.gov/sites/default/files/documents/2012/january/competes_010511_0.pdf (finding that three factors that form the basis of a strong innovative environment are support for education, research, and infrastructure); THOMAS SOWELL, BASIC ECONOMICS: A COMMON SENSE GUIDE TO THE ECONOMY 301-02 (Basic Books 4th ed. 2011) (discussing the importance of capital markets to support entrepreneurial activity); CHARLES SCHULTZE, MEMOS TO THE PRESIDENT: A GUIDE THROUGH MACROECONOMICS FOR THE BUSY POLICYMAKER 304 (1991) (suggesting that more engineering degrees leads to greater development of useful ideas); Wesley M. Cohen et al., *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (Or Not),* NAT'L BUREAU OF ECON. RESEARCH, WORKING PAPER NO. 7552 at 11 (2000), *available at* http://www.nber.org/papers/w7552.pdf ("secrecy and lead time are ranked comparably

In essence, a trade secret is information that derives value from not being known to competitors. Trade secrets play a critical role in supporting innovation in the United States. For example, in one study, secrecy ranked first or second in importance for product innovations in "twenty-four of the thirty-three surveyed industries."[6] Trade secret law particularly favors small companies, which tend to be engines of innovation, because the hurdles to obtaining trade secret protection are relatively low.[7] In contrast to patent law, trade secrets require only reasonable efforts at secrecy from the trade secret holder to earn legal protection.[8] Moreover, trade secret protection may potentially last forever.[9]

Trade secret law, however, like other areas of intellectual property law, must strike a careful balance. Too little protection results in inadequate incentives to develop useful information and wasteful expenditures on protection.[10] Too much protection causes harm in a number of different ways. By granting too much of a monopoly on trade secret information, trade secret law prevents companies from competing to provide better products using that information.[11] Over-protection also decreases worker mobility by preventing employees with knowledge of their employers' trade secrets from departing to work for competitors or to start their own companies.[12] This restricts personal freedom and economic dynamism. Monopolies on trade secret information inhibit follow-on innovation, a problem because most innovation builds on innovation.[13] Finally, over-broad trade secret law limits free speech and restricts the flow of information important to the public.[14] For example, natural gas companies

---

overall as the two most effective appropriability mechanisms for product innovations") [hereinafter Cohen].

[6] Cohen, *supra* note 5, at 13.

[7] *See* Cohen, *supra* note 5, at 7, 14-16; *see also* Richard C. Levin et al., *Appropriating the Returns from Industrial Research and Development*, 18 BROOKINGS PAPERS ON ECON. ACTIVITY 783 (1987); CHI RESEARCH, INC., SMALL BUS. ADMIN., SMALL SERIAL INNOVATORS: THE SMALL FIRM CONTRIBUTION TO TECHNICAL CHANGE 3 (2003), *available at* http://www.sba.gov/advo/research/rs225tot.pdf (small businesses develop thirteen times more patents per employee than large businesses).

[8] *See* UNIF. TRADE SECRETS ACT § 1(4)(ii), 14 U.L.A. 433 (1985); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 313 (2008) [hereinafter *Surprising Virtues*].

[9] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 494 (1974) (Marshall, J., concurring) (noting that trade secret law offers protection of unlimited duration).

[10] *See infra* Part I.B.

[11] *See infra* Part I.B.

[12] *See infra* Part I.B.

[13] *See infra* Part I.B.

[14] *See infra* Part I.B.

shield information about their potentially dangerous hydraulic fracturing practices from regulators and the public by arguing that they are trade secrets.[15]

The rhetoric among political leaders on trade secret cyber-misappropriation ignores this delicate balance of conflicting policy concerns. An otherwise obscure area of the law, trade secrets have been the subject of an unprecedented level of attention recently due to concerns about cyber-hacking. President Obama, high-ranking members of his administration, and members of Congress have all loudly voiced concern.[16] Fueled in part by national security concerns about the cyber-hacking of military secrets, the rhetoric from these political leaders has tended to be alarmist, protectionist, and moralistic.

This one-sided concern with protecting trade secrets is leading to a dramatic strengthening of trade secret law. The Obama administration is now conducting a legislative review to determine if more legislation is needed to enhance enforcement against trade secret theft.[17] And a number of parties are advocating strengthening civil trade secret law by federalizing it. Indeed, four bills have recently been proposed in Congress to federalize

---

[15] Travis D. Van Ort, *Hydraulic Fracturing Additives: A Solution to the Tension Between Trade Secret Protection and Demands for Public Disclosure*, 4 KY. J. EQUINE, AGRIC. & NAT. RESOURCES L. 439, 440, 458 (2012); Mike Soraghan, *In Fracking Debate, 'Disclosure' is in the Eye of the Beholder,* N.Y. TIMES (June 21, 2010), http://www.nytimes.com/gwire/2010/06/21/21greenwire-in-fracking-debate-disclosure-is-in-the-eye-of-19087.html.

[16] *See, e.g.*, Pres. Barack Obama, Remarks by the President on Securing our Nation's Infrastructure (May 29, 2009), a*vailable at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure; Gen. Keith B. Alexander, Director, National Security Agency, Keynote Address at American Enterprise Institute on Cybersecurity and American Power (July 9, 2012), *available at* http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/; 159 CONG. REC. S3165-66 (daily ed. May 7, 2013) (statement of Sen. Carl Levin); *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology Before the H. Subcomm. on Oversight and Investigations,* 113th Cong. (July 9, 2013) (statement of Tim Murphy, H. Rep.), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/OI/20130709/HHRG-113-IF02-MState-M001151-20130709.pdf; *Chinese Telecommunications Investigation Open Hearing Before the H. Permanent Select Comm. on Intelligence*, 112th Cong. (2012) (Opening Statement of Dutch Ruppersberger, H. Rep., Md., 2nd Cong. Dist.), *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/09122012DutchOpening.pdf.

[17] OFFICE OF THE PRESIDENT OF THE UNITED STATES, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 12 (Feb. 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [hereinafter ADMINISTRATION STRATEGY].

civil trade secret law by adding a private right of action to the Economic Espionage Act (EEA).[18] This would significantly increase the rights of those wishing to protect information.

Strengthening trade secret law, however, will likely do little to combat cyber-misappropriation. This paper uses an array of studies of cyber-risks and trade secret litigation to show that trade secret holders cannot and will not pursue cyber-misappropriators in court for technological and business reasons, not for legal reasons. Worse, strengthening trade secrets will cause significant collateral damage. Trade secret holders will use stronger trade secret rights in other types of misappropriation cases in ways that will impede follow-on innovation, restrict worker mobility, dampen competition, and hamper public access to useful information, including for purposes of free speech. In short, the political rhetoric ignores the fact that the costs outweigh the benefits of bolstering trade secret law to respond to cyber-misappropriation of trade secrets.

The argument is set forth in the following three parts. Part I outlines trade secret doctrine and policy, explaining how trade secret doctrine balances conflicting policy concerns. Part II discusses the cybersecurity threat to American trade secrets and the political response. This part shows how the political rhetoric has linked protecting trade secrets to emotionally resonant issues, including national security and job loss, and is leading to the strengthening of trade secret law. Part III shows how expanding trade secret rights, particularly by adding the private party right of action under the EEA, would likely harm innovation as well as other policy interests.

I. TRADE SECRET LAW

Trade secret law in America has its origins in 19th century state common law.[19] In 1837, a Massachusetts court issued the first known American opinion recognizing limited rights in secret information.[20] By 1939, the American Law Institute had identified a set of commonly

[18] Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014); Future of American Innovation and Research Act of 2013, S. 1770, 113th Cong. (2013); Private Right of Action Against Theft of Trade Secrets Act of 2013, H.R. 2466, 113th Cong. (2013); Protecting American Trade Secrets and Innovation Act of 2012, S. 3389, 112th Cong. (2012).

[19] MELVIN F. JAGER, 1 TRADE SECRETS LAW § 2.3 (2013) (recounting the development of trade secret law).

[20] Vickery v. Welch, 36 Mass. (1 Pick.) 523, 526 (1837) (enforcing a covenant to sell rights to a secret art of making chocolate); *Surprising Virtues*, *supra* note 8, at 316.

accepted principles of trade secret law in the First Restatement of Torts.[21] In 1979, in response to the lack of uniformity among states' common law and ambiguity on some legal issues, the ALI promulgated the Uniform Trade Secrets Act (UTSA).[22]

Now, all U.S. states and the District of Columbia have adopted the UTSA in some form, except for New York and Massachusetts.[23] Despite these holdouts and some variations in the version of the UTSA adopted, civil trade secret law is largely the same across the country.[24]

Trade secret rights tend to be protected through this civil law. Although there is a federal criminal law addressing trade secrets and many states have criminal trade secret statutes,[25] trade secret rights are rarely enforced through criminal law. Only about two percent of state trade secret cases resulting in an appellate opinion involve a state criminal trade secret statute.[26] On the federal level, trade secret misappropriation is prosecuted through the Economic Espionage Act.[27] However, these cases are infrequent. Substantive trade secret law in the courts is almost always state

---

[21] RESTATEMENT (FIRST) OF TORTS §§ 757-59 (1939); JAMES POOLEY, TRADE SECRETS § 2.02[1] (2000) (stating that for over forty years after its publication in 1939, the Restatement (First) of Torts "was almost universally cited by state courts, and in effect became the bedrock of modern trade secret law").

[22] *See* UNIF. TRADE SECRETS ACT (amended 1985) prefatory note, 14 U.L.A. 433, 434 (1990) (noting the "undue uncertainty concerning the parameters of trade secret protection" and the "confused status" of the law); *see also* Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Following the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 502-20 (2010) (providing a detailed account of the drafting of the UTSA). The ALI issued a revised version in 1985. *See id.*

[23] *See* 1 MELVIN F. JAGER, TRADE SECRETS LAW § 3:29, n.1 (2013) (providing citations to statutes enacting the UTSA in 47 states and the District of Columbia). Texas enacted Texas Senate Bill 953 on May 3, 2013, after this version of the Jager text was printed. The bill went into effect on September 1, 2013. However, some states, particularly North Carolina and Alabama, have adopted versions of the statute which vary significantly from the UTSA. *See* Marina Lao, *Federalizing Trade Secrets Law in an Information Economy*, 59 OHIO ST. L.J. 1633, 1657 (1998).

[24] *See* JAMES POOLEY, TRADE SECRETS § 2.03[7](c) (2013) ("It is true that the similarities in substance among state enactments are far greater than the differences in language used.") Even where the language of the law differs, courts' interpretations are similar. *See id.* at § 2.01[1] ("Usually what is seen as 'improper means' in Illinois will be similarly seen in California . . . .")

[25] *See* 18 U.S.C. § 1831 et seq. (federal criminal statute); 1 MELVIN F. JAGER, TRADE SECRETS LAW, app. L3 (1990) (providing state criminal statutes).

[26] David S. Almeling, et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 76 (2010-2011) [hereinafter *State Study*].

[27] 18 U.S.C. §§ 1831 et seq.

law.[28] As a result, this paper will focus its discussion of trade secret law on the UTSA as broadly representative of trade secret law across the states.

A. Trade Secret Doctrine

Proving a claim of trade secret misappropriation essentially requires establishing two elements: that the plaintiff possesses a trade secret and that the trade secret has been misappropriated.[29] With regard to the trade secret element, a trade secret is "information . . . that derives independent economic value . . . from not being generally known to [and not] readily ascertainable by . . . [those] who can obtain economic value from its disclosure or use."[30] Thus, trade secrets must not only be secret, they must derive economic value from being secret—essentially a competitive advantage.[31] Trade secrets, as a result, are not subject matter specific. The information protected by trade secret law may constitute any information as long as it is valuable because it is secret.[32]

In addition, to merit protection as a trade secret, the information at issue must be subject to reasonable efforts to maintain its secrecy.[33] What constitutes reasonable efforts, of course, lends itself to different interpretations. Courts vary as to the level of effort necessary to adequately protect a trade secret.[34]

The second element, misappropriation, requires the acquisition of a trade secret by some form of improper means or the use or disclosure of a trade secret in breach of a confidence.[35] These two forms of

---

[28] David S. Almeling, et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 45 GONZ. L. REV. 291, 306 (2009-2010) [hereinafter *Federal Study*]. Finally, some courts have interpreted the Computer Fraud and Abuse Act ("CFAA") to apply to cases involving hacking computer systems to take proprietary data. *See* Zoe Argento, *Whose Social Network Account? A Trade Secret Approach to Allocating Rights*, 19 MICH. TELECOMM. & TECH. L. REV. 201, 258 n.307 (2013), *available at* http://www.mttlr.org/volnineteen/argento.pdf. However, this approach to the CFAA is controversial. *See id.*

[29] *See* 1 MELVIN JAGER, TRADE SECRETS LAW § 5:5 (2013) (Jager further divides the misappropriation inquiry into two separate elements).

[30] *See* UNIF. TRADE SECRETS ACT § 1(4)(i).

[31] *See id.*

[32] *See id.*

[33] *See id.* at § 1(4)(b).

[34] *See* Note, *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 463-64 (1992) (discussing the requirement of reasonable security precautions).

[35] *See* UNIF. TRADE SECRETS ACT § 1(2); *Surprising Virtues*, *supra* note 8, at 318-19. The UTSA also imposes liability for knowingly using or disclosing a trade secret from a third

misappropriation—improper means and breach of confidence— correspond roughly to two different sets of circumstances in which trade secrets are taken, respectively, misappropriation by outsiders and misappropriation by insiders.[36]

Misappropriation by outsiders generally occurs in the context of competitors seeking business intelligence.[37] These cases define rights between strangers and tend to sound in tort law.[38] Improper means include not only actions that would be wrongful in themselves, such as theft, but also calculated efforts to overcome reasonable secrecy measures.[39] Notably, the UTSA specifically includes "espionage through electronic or other means" as a form of improper means.[40] This has been interpreted to cover acquiring trade secrets through hacking into computer systems.[41]

In contrast, misappropriation by insiders typically involves parties to a business relationship, such as departing employees, and tends to sound in contract.[42] In these cases, misappropriation depends on whether the defendant breached an agreement of confidentiality.[43] The agreements may be explicit, for example, in the form of nondisclosure agreements. They may also be implied. In the case of employees, the confidentiality agreement is sometimes implied based on the employee's tacit understanding of her employment obligations.[44]

---

party who acquired the trade secret through improper means or a breach of confidence. *See* UNIF. TRADE SECRETS ACT § 1(2)(ii)(B).

[36] *See Surprising Virtues*, *supra* note 8, at 318-19.

[37] *Id.* at 317.

[38] *See id.*

[39] *See* UNIF. TRADE SECRETS ACT § 1(1); E.I. DuPont De Nemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970).

[40] UNIF. TRADE SECRETS ACT § 1(1).

[41] *See, e.g.*, Physicians Interactive v. Lathian Systems, Inc., 2003 WL 23018270, *8 (E.D. Va. 2003) ("There can be no doubt that the use of a computer software robot to hack into a computer system and to take or copy proprietary information is an improper means to obtain a trade secret, and thus is misappropriation under the VUTSA."); *see also* Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1326 (S.D. Fla. 2003) (finding that hacking into a computer system constitutes misappropriation by espionage through electronic means).

[42] *See Surprising Virtues*, *supra* note 8, at 317.

[43] *See id.*

[44] *See, e.g.*, Am. Bldg. Maint. Co. v. ACME Prop. Servs., 515 F. Supp. 2d 298, 310 (N.D.N.Y. 2007) ("[Under New York law,] former employees can be restricted from using their former employer's trade secrets to advance their own interests, even when they have not signed an employment agreement limiting their activities."); Premier Lab Supply, Inc. v. Chemplex Indus. Inc., 10 So. 3d 202, 206 (Fla. Dist. Ct. App. 2009) (holding lack of a confidentiality agreement with an employee to whom confidential information is disclosed does not by itself defeat trade secret status for the information because an employee who

The correlation of outsiders with misappropriation by improper means and insiders with misappropriation by breach of confidence is not perfect, of course. Insiders may use their existing access to improperly hack into trade secrets to which they were not granted access, and outsiders may acquire trade secrets through unintended disclosure on the part of the trade secret holder.[45] However, as the statistics show, insiders in trade secret cases tend to exploit access granted them in breach of a confidentiality agreement whereas outsiders tend to acquire trade secrets through some form of improper means unrelated to a breach of confidence.[46]

Likewise, both breaches of confidence and improper means may be accomplished through computer systems. The exploitation of internet access that has provoked the most public concern recently is the hacking of a trade secret holder's computer system by outsiders, especially foreign governments.[47] An insider, however, may use her authorized access to the employer's computer system to obtain her employer's trade secrets. Then, she might use her internet access to send the information to a new employer. For purposes of consistency, this paper will refer to the acquisition of trade secrets by wrongfully circumventing barriers to access in computer system as cyber-misappropriation, whether conducted by insiders or outsiders. Cyber-misappropriation, in brief, will refer to acquisition by hacking, and not the use of computer systems for other forms of use and disclosure of the trade secret.[48]

B. Theory and Goals of Trade Secret Law

The rationale for trade secret rights does not have the coherent policy basis of other areas of intellectual property, particularly patent and

---

acquires a special technique or process in his employment is, as a matter of law, under a duty not to use it for his own benefit or disclose it to others).

[45] *See* UNIF. TRADE SECRETS ACT § 1(2).

[46] Verizon reported that most cases of insider data breach involve insiders misusing their privileges. VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 6 (2013) ("Correlated with the 14% of breaches tied to insiders, privilege misuse weighs in at 13%."), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf [hereinafter VERIZON 2013 REPORT]; PRICEWATERSHOUSECOOPERS, KEY FINDINGS FROM THE 2013 US STATE OF CYBERCRIME SURVEY CERT STUDY 10 (June 2013), *available at* http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf [hereinafter CERT 2013 SURVEY].

[47] *See infra* note 145.

[48] I refer to the definition of "hacking" in the Free Dictionary: "To use one's skill in computer programming to gain illegal or unauthorized access to a file or network." Free Dictionary *available at* http://www.thefreedictionary.com/hacking.

copyright, which rest firmly on an incentive theory set forth in the Constitution.[49] Trade secret law evolved from torts based on differing rationales such as breach of confidence, unfair competition, and trespass to property.[50] These jumbled roots have led some commentators to describe trade secret law as a "doctrine in search of a justification."[51] However, the more constructive way to describe the theoretical basis of trade secret law is that it consists of multiple theories, each of which tends to pull in the same direction. The two principal theories upon which trade secret law rests are tort theory and property theory.[52]

The tort theory bases trade secret rights on the goal of discouraging undesirable conduct. The older version of this approach focuses on maintaining standards of business morality, while the modern version seeks to discourage unfair competition.[53] Both versions, however, aim to discourage behavior that leads to wasteful efforts to protect trade secrets against discovery.[54] As the Fifth Circuit observed, "Our tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened."[55] The Restatements, UTSA, and most state courts rely on the tort theory as the justification for trade secret rights.[56]

---

[49] *See* U.S. CONST. art. I, § 8, cl. 8; *see also* Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989, 993-1000 (1997).
[50] *Surprising Virtues*, *supra* note 8, at 316.
[51] *See, e.g.*, Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 243 (1998).
[52] *See, e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974) ("The maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law."); RESTATEMENT (THIRD) UNFAIR COMPETITION § 39 cmt. b. (noting that courts both justify trade rights on a property theory and a theory of improper conduct).
[53] *See* Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 886-89 (2002).
[54] E. I. DuPont De Nemours & Co. v. Christopher, 431 F.2d 1012, 1016-17 (5th Cir. 1970). Similarly, the Supreme Court noted that trade secret law serves the purpose of avoiding "detrimental misallocation of resources and economic waste." Kewanee Oil Co., 416 U.S. at 487.
[55] E. I. DuPont De Nemours & Co., 431 F.2d at 1016.
[56] *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939) (rejecting the property theory in favor of a general duty of good faith); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 reporters' note, cmt. b, 440 (1995) (listing cases); UNIF. TRADE SECRETS ACT § 1 commissioners' cmt. (amended 1985), 14 U.L.A. 438 (1990) ("One of the broadly stated policies behind trade secret law is 'the maintenance of standards of commercial ethics.'"); 1 MELVIN F. JAGER, TRADE SECRETS LAW §§ 1:3, 1:3 n.16 (noting that standards of fairness and commercial morality continue to be the touchstone of trade secret law in the courts and listing cases).

The property theory views trade secrets as a form of intellectual property, like patents or copyright.[57] The Supreme Court, in particular, identified trade secrets as a form of property in *Ruckelshaus v. Monsanto*, rejecting its earlier view that trade secret rights rested purely on a commercial morality justification.[58] Commentators and several state courts have also accepted this view.[59]

Under this approach, trade secret rights serve the purpose of providing incentives to develop useful and innovative information by granting rights in that information.[60] The reasoning proceeds as follows. New and valuable information is often costly to develop. A new chemical formula or engineering process, for example, may take years and significant skill to create. As a result, rational actors will not engage in this investment of time and money without hope of compensation for their efforts. Trade secrets, however, are merely information and are therefore easily copied.[61] The original developer of the useful information loses the competitive advantage that the information gives her when her competitors copy and use the information, too. This deprives the developer of the incentive to invest in developing it in the first place. By granting legal protection from misappropriation, trade secret law preserves the incentive to invest in developing useful information.[62]

A number of authorities rely on the tort and property approaches simultaneously. The Supreme Court, for example, identified both theories as justification for trade secret law in *Kewanee Oil Company v. Bicron*

---

[57] *See, e.g.*, *Surprising Virtues*, *supra* note 8, at 329 ("Trade secrets are best understood not as applications or extensions of existing common law principles (warranted or unwarranted), but as IP rights.")

[58] Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1004, n.9 (1984). The Court argued that its earlier decision in *E.I. DuPont De Nemours Powder Co. v. Masland* did not deny the existence of a property interest in trade secrets but merely stood for the proposition that a property interest was unnecessary to decide the case. *Id.* Nevertheless, Justice Holmes's statement in *Masland*—"The property may be denied, but the confidence cannot be."—seems to be a fairly clear rejection of the property theory. 244 U.S. 100, 102 (1917).

[59] *See, e.g.*, *Surprising Virtues*, *supra* note 8, at 312 (rejecting other theories of trade secret law in favor of a property theory); Union Carbide Corp. v. Tarancon Corp., 742 F. Supp. 1565, 1579 (N.D. Ga. 1990) (Georgia); Jensen v. Redevelopment Agency, 998 F.2d 1550, 1556 (10th Cir. 1993) (Utah).

[60] *See e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481-82 (1974).; *Surprising Virtues*, *supra* note 8, at 330.

[61] As Thomas Jefferson stated: "That ideas should freely spread from one to another over the globe. . . seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space . . . ." Letter from Thomas Jefferson to Isaac McPherson (Aug. 13, 1813), *available at* http://press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html.

[62] *See Surprising Virtues*, *supra* note 8, at 329-30.

Corporation: "The maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law."[63] As Judge Posner observed, the two theories are complementary. Both aim to encourage wealth creation rather than mere redistribution.[64]

Under either theory, trade secret law must balance conflicting policy concerns. In setting the right standard for conduct under the tort theory, trade secret law must balance the promotion of healthy competition and innovation against the discouragement of inefficient over-investment in self-protection. The public, as a whole, loses when companies devote their resources to protecting their ideas from each other.[65] However, the public also suffers when companies do not compete vigorously with each other.[66] Granting an overbroad monopoly on information prevents companies from competing to produce better products and services based on that information.[67]

The tension between encouraging competition and discouraging waste is particularly salient when employees are privy to their employers' trade secrets. Employees may take those trade secrets to a competitor when they leave to find a new job. Concern over this possibility may cause the first employer not to fully exploit the trade secret because it fears disclosing the information to its workers.[68]

Restricting employees from leaving also leads to harmful consequences. First, the public interest in open competition suffers when

---

[63] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974).
[64] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178–79 (7th Cir. 1991).
[65] Kewanee Oil Co., 416 U.S. at 487 ("In addition to the increased costs for protection from burglary, wire-tapping, bribery, and the other means used to misappropriate trade secrets, there is the inevitable cost to the basic decency of society when one firm steals from another.")
[66] *See* Wexler v. Greenberg, 160 A.2d 430, 435 (Pa. 1960) (noting that "society suffers when competition is diminished by slackening the dissemination of ideas, processes and methods."); THOMAS SOWELL, BASIC ECONOMICS: A COMMON SENSE GUIDE TO THE ECONOMY 157 (Basic Books 4th ed. 2011) (explaining how competition reduces prices for consumers); JOHN M. LEVY, ESSENTIAL MICROECONOMICS FOR PUBLIC POLICY ANALYSIS 52 (Praeger Publishers 1995) (competition promotes product innovation and product differentiation).
[67] *See* Brunswick Corp. v. Outboard Marine Corp., 404 N.E.2d 205, 207 (Ill. 1980) (noting the public interest in the production of goods unprotected by a valid patent); *see also* Willard K. Tom & Joshua A. Newberg, *Antitrust and Intellectual Property: From Separate Spheres to a Unified Field*, 66 ANTITRUST L.J. 167, 171 (1997) (stating that "ownership of intellectual property confers upon the intellectual property holder a 'monopoly'").
[68] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485-86 (1974).

workers are prevented from competing with former employers.[69] Second, when employees cannot leave, employers do not compete for the best employees either through compensation or hiring.[70] The worker then has little incentive to improve her skills because she will not be compensated for her investment through competition among employers.[71] A number of undesirable consequences result, including reduced innovation, productivity, and economic growth.[72]

Restricting employee mobility also decreases innovation by impeding the sharing of ideas. When allowed to move from one employer to another, employees with skills obtained in one company bring new perspectives and solutions to the next company. And the former employer benefits from the reciprocal effect; workers leave other companies to join it, also bringing fresh ideas with them.[73] As Ronald Gilson explains, these knowledge spillovers spark a cascade of innovation, continually rejuvenating the local economy.[74] The cross-pollination effect helps to explain the sustained productivity of hotbeds of innovation, like Silicon Valley.[75]

The property theory implicates a related set of conflicting policies. Under the property theory, trade secret law balances providing incentives to

---

[69] *See* Wexler v. Greenberg, 160 A.2d 430, 433 (Pa. 1960) (noting that preventing a worker from using his skills for another employer may harm "the public in general in forestalling, to any extent widespread technological advances").

[70] *See* ORLY LOBEL, TALENT WANTS TO BE FREE 31-38 (Yale University Press 2013); Catherine Fisk & Adam Barry, *Contingent Loyalty and Restricted Exit: Commentary on the Restatement of Employment Law*, 16 EMP. RTS. & EMP. POL'Y J. 413, 34 (2013), *available at* http://ssrn.com/abstract=2060621 ("Studies of how companies motivate employees today emphasize that, rather than focusing on how to prevent valuable employees from leaving, successful employers implement strategies that encourage them to stay.").

[71] *Id.* at 28 ("[E]mployees in strict enforcement jurisdictions will be discouraged from investing in their human capital because they know that they will not be able to solicit employment offers from outside firms that they could either accept or use as leverage to negotiate an increase in their salary at their current employer.").

[72] *Id.* at 26, 28-30, 35 (restraining employees' ability to compete depresses innovation by impeding the cross-pollination of skills and ideas between organizations, hampers the creation of new firms and entrepreneurial activity, and increases employer search costs).

[73] Anders Malmberg & Dominic Power, (*How) Do (Firms in) Clusters Create Knowledge?*, 12 INDUS. & INNOVATION 409, 410 (2005); *see generally* ORLY LOBEL, *supra* note 70 (explaining how the economy benefits when workers are free to move between employers).

[74] Robert H. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants not to Compete*, 74 N.Y.U. L. REV. 575, 584-86 (1999) (explaining that knowledge spillovers between firms leads to the development of new products that "reset the industry life cycle").

[75] *Id.* at 590-92 (noting that high employee mobility helps to explain why Silicon Valley has experienced the development of new industry after new industry).

develop useful and innovative information against public access to that information. Although the public benefits when companies use their trade secrets to provide better products and services, the public would benefit more directly by having access to the trade secrets themselves.

In particular, allowing the trade secret holder exclusive rights to use a trade secret inhibits follow-on innovation. This can slow progress, because innovation tends to build on previous innovation.[76] Indeed, most technology, from computers to pharmaceutical drugs, is the outcome of a long chain of individual innovations.[77] When more people have access to useful information, especially competitors trained in that area of technology, more people can build upon that information with new innovations. As discussed above, public access to innovation also enhances competition. Finally, trade secret information is vital to many other public interests, such as free speech, safety, and health.[78]

To balance these conflicting concerns, trade secret law grants only a limited and porous protection to trade secrets. As the Supreme Court observed, "trade secret law functions relatively as a sieve."[79] Trade secrets are allowed to leak to the public in four principal ways.

First, other parties may divine a trade secret through reverse engineering without fear of liability for misappropriation.[80] Reverse engineering is the process of figuring out how a product works, often by working backwards from the known product to determine the process of its manufacture.[81] Competitors benefit most directly from the reverse engineering exception to misappropriation because many trade secrets are

---

[76] *See, e.g.*, Jeffrey L. Furman & Scott Stern, *Climbing Atop the Shoulders of Giants: The Impact of Institutions on Cumulative Research*, AM. ECON. REV. 101(5) (2011): 1933–1963 (noting the general observation that innovation builds on innovation and showing an example in the case of biological resource centers).

[77] As Sir Isaac Newton famously observed: "If I have seen farther, it is by standing on the shoulders of giants." STEPHEN HAWKING, *Isaac Newton (1642-1727): His Life and Work*, *in* ON THE SHOULDERS OF GIANTS 725 (Stephen Hawking ed., 2002).

[78] *See infra* notes 99-106 and accompanying text.

[79] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 490 (1974).

[80] *See* UNIF. TRADE SECRETS ACT, Comment to § 1 ("Proper means include: . . . Discovery by 'reverse engineering', that is, by starting with the known product and working backward to find the method by which it was developed.") However, courts have accepted the principle of reverse engineering as a form of proper means to acquire a trade secret for more than a century. *See, e.g.*, Tabor v. Hoffman, 23 N.E. 12, 13 (1889); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974); Craig L. Uhrich, *The Economic Espionage Act-Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. & TECH. L. REV. 147, 167, n.160 (2001).

[81] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974); EILAM, ELDAD & CHIKOFSKY, ELLIOT J., REVERSING: SECRETS OF REVERSE ENGINEERING 3 (John Wiley & Sons 2007).

too complicated for the average member of the public to reverse engineer.[82] The public, however, benefits in the long run because competitors use the information to compete with the original trade secret holder in providing better goods and services to the public. Additionally, access by competitors provides more scope for follow-on innovation.

A second type of leakage takes place through departing employees. Although an employee is liable for misappropriation if she knowingly takes her employer's trade secrets with her when she leaves, she may take general and industry-specific knowledge, even if she learned it on the job.[83] For example, a welder may take the general welding skills she learned in her previous employment to a new employer, but she cannot take her knowledge of her employer's trade secret on the welding compound.

The line between trade secrets and unprotected general and industry-specific knowledge, however, can be blurry.[84] The definition of a trade secret itself is imprecise. What constitutes "reasonable" efforts to maintain secrecy and "readily ascertainable" are but two of the issues in establishing the existence of a trade secret that call for close line-drawing by the courts.[85] In addition, as an evidentiary matter, it may be difficult to prove that an employee took purely tacit knowledge.[86] An employer can prove

[82] That reverse engineering of trade secret must be challenging is a necessary consequence of the requirement that a trade secret not be "readily ascertainable." *See* UNIF. TRADE SECRETS ACT § 1(4)(i). If information was very easy to obtain through reverse engineering, then it likely would not qualify as a trade secret because it would be "readily ascertainable." *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f.

[83] *See* Basic Chems., Inc. v. Benson, 251 N.W.2d 220, 227 (Iowa 1977) ("One rather salient point runs steadfastly throughout decisions in this area in most jurisdictions, and that is that the employee, upon terminating his employment relationship with his employer, is entitled to take with him 'the experience, knowledge, memory, and skill, which he had gained while there employed."); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 cmt. d (1995) ("The distinction between trade secrets and general skill, knowledge, training, and experience is intended to achieve a reasonable balance between the protection of confidential information and the mobility of employees.").

[84] *See* Gilson, *supra* note 74, at 598-99.

[85] *See* UNIF. TRADE SECRETS ACT § 1(4); *Surprising Virtues*, *supra* note 8, at 317.

[86] Some courts have adopted the inevitable disclosure doctrine, but this is controversial and rejected by many courts. Under the inevitable disclosure doctrine, a former employee may be enjoined from working for a competitor because the court determines that she would inevitably user her former employer's trade secrets for the benefit of her new employer in the course of her work. *See, e.g.*, Pepsico, Inc. v. Redmond, 54 F.3d 1262, 1269 (7th Cir. 1995) (enjoining a former employee from working for a competitor on the grounds that he would necessarily make decisions for his new employer by relying on his knowledge of his former's employer's trade secrets). A number of courts have rejected this doctrine as too restrictive of employee mobility. *See, e.g.*, Campbell Soup Co. v. Giles, 47 F.3d 467, 469 (1st Cir. 1995) (affirming district court's refusal to grant preliminary injunction restraining former employee from working for competitor); Cudahy Co. v. American Labs., Inc., 313

misappropriation fairly easily when an employee takes stacks of documents containing trade secrets.[87] The employer faces a greater challenge in proving that the employee took trade secrets stored only in her head. Furthermore, courts hesitate to protect information as trade secrets that cannot be easily distinguished from a worker's general skill and knowledge.[88] As the Third Restatement of Unfair Competition observes: "[w]hen a former employee uses information from memory rather than from physical records taken from the former employer, courts may be more likely to regard the information as part of the employee's general knowledge and experience."[89] Finally, due to the many uncertainties in a trade secret claim, trade secret litigation tends to be expensive.[90] An employer may therefore hesitate to bring suit in a case involving close issues of general or industry-specific knowledge, thereby allowing some trade secrets to leak out with departing employees.[91]

But again, this seepage of useful information benefits the public. When employees have the option of leaving, employers must compete to retain the best workers. This gives employees more incentive to perform well and to invest in professional self-improvement.[92] In addition, the cross-pollination effect above leads to greater innovation, to the benefit of the economy and the public.[93]

A third way in which trade secret law allows information to leak to the public is through innocent discovery.[94] The UTSA and the common law

---

F. Supp. 1339, 1343 (D. Neb. 1970) (noting absence of covenant not to compete in dismissing unfair business practice claim).

[87] *See, e.g.*, ONCIX 2011 Report, *infra* note 113, at 2 (defendant arrested with 250,000 pages of proprietary information in his house).

[88] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 cmt. d (1995).

[89] *Id.*

[90] Gilson, *supra* note 74, at 599; SHARON SANDEEN & ELIZABETH ROWE, TRADE SECRET LAW IN A NUTSHELL § 4.12.3 (West 2013); American Intellectual Property Law Association, 2013 Report of the Economic Survey (2013), *available at* http://www.patentinsurance.com/custdocs/2013AIPLA%20Survey.pdf.

[91] Gilson, *supra* note 74, at 600. The trade secret holder can remedy this problem in part by requiring employees to sign noncompete agreements restricting departing employees from competing with the employer until such time as any trade secret the departing employee knows becomes obsolete. Not all states enforce such agreements, however. *See* CAL. BUS. & PROF. CODE § 16600 (making non-compete agreements unenforceable in California). Most states allow courts to strike down or revise such agreements if they seem unreasonable, which leads to more expensive litigation. *See* Viva Moffat, *Making Non-Competes Unenforceable*, 54 ARIZ. L. REV. 939, 943-51 (2012).

[92] *See* Fisk & Barry, *supra* note 70, at 33.

[93] *See* Gilson, *supra* note 74, at 591.

[94] *See* Kewanee Oil Co., 416 U.S. at 476.

do not impose liability for learning of a trade secret without notice that it is secret.[95]

Fourth, the courts allow the disclosure of trade secrets to serve other compelling public interests. Trade secret common law generally recognizes a privilege to disclose trade secrets "in connection with . . . information that is relevant to public health or safety, or to the commission of a crime or tort, or other matters of substantial concern."[96] One such interest is free speech. In *CBS v. Davis*, for example, the Supreme Court held that enjoining the disclosure of trade secrets was an unconstitutional prior restraint of free speech.[97] Justice Blackmun found in *CBS* that the economic harm that would allegedly result from a television broadcast of trade secrets did not justify a prior restraint on speech.[98] Numerous other courts have also held that preliminary injunctions against public disclosure of trade secrets bear a heavy presumption against validity because of the First Amendment concerns.[99]

Another such interest is justice. For example, courts have recognized a privilege to disclose trade secrets for the purpose of revealing criminal fraud.[100] Assorted state federal statutes and regulations privilege the disclosure of trade secrets to serve a variety of other public concerns, such as the environment,[101] health and safety,[102] and unmasking corporate wrongdoing through whistleblowing.[103]

---

[95] *See* UNIF. TRADE SECRETS ACT § 1(2)(ii)(C); RESTATEMENT (FIRST) OF TORTS § 758.

[96] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1993) ("[D]isclosure of another's trade secret for purposes other than commercial exploitation may implicate the interest in freedom of expression or advance another significant public interest. . . . The existence of a privilege to disclose another's trade secret depends upon the circumstances of the particular case, including the nature of the information, the purpose of the disclosure, and the means by which the actor acquired the information.").

[97] 510 U.S. 1315, 1316 (1994). In *CBS*, the Supreme Court stayed a preliminary injunction preventing a television station from broadcasting footage of allegedly proprietary meat packing processes in an exposé on the beef processing industry. *Id.*

[98] CBS, Inc. v. Davis, 510 U.S. at 1317-18.

[99] *See* Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 811 n.212 (2007).

[100] Re v. Horstmann, C.A. 83C-FE-82, 1987 WL 16710, at *1-2 (Del. Super. Ct. Aug. 11, 1987) (recognizing a privilege to disclose to law enforcement officials trade secrets relevant to criminal fraud that had been disclosed to the defendants in confidence, citing the former Restatement).

[101] Several states have passed statutes and regulations requiring companies engaging in hydraulic fracturing, a method of extracting natural gas, to provide information on the process to regulators, even when that information includes trade secrets. *See, e.g.*, 2 COLO. CODE REGS. 404-1:205A(b)(2)(B); ARK. CODE R. 178.00.1-B-19(l)(8). Some states even require information that qualifies for trade secret protection be disclosed to the public. *See, e.g.*, 2 COLO. CODE REGS. 404-1:205A(d).

Finally, once a trade secret enters the public domain, whether legitimately or through misappropriation, it cannot be reclaimed.[104] The secrecy requirement for trade secret protection ensures that no one wins protection for information already in the public domain. Relatedly, the requirement of reasonable efforts to maintain secrecy prevents the trade secret holder from allowing the information to flow to competitors at one time and then later suing them for trade secret misappropriation.[105] In addition, if the information subject to trade secret protection is developed independently by a third party and becomes common knowledge, the information loses all trade secret protection.[106]

II. CYBER-RISKS: CYBER-MISAPPROPRIATION AND POLITICAL REACTIONS

A. The Cyber-Misappropriation Threat

Numerous studies indicate that cyber-misappropriation of trade secrets is a serious and growing threat. First, economic and technological trends make misappropriation easier and more lucrative. Second, cyber-hackers have become better financed and organized. This is particularly true of the hackers sponsored by nation states. China has made taking competitive information, particularly American competitive information, a matter of national policy. It appears that other countries have also entered this game. Unsurprisingly, the increasing sophistication of the hackers has led to more potent attacks, such as the insidious long-term cyber-intrusions known as advanced persistent threats. Finally, the available statistics on cyber-misappropriation, although deficient in many respects, suggest that cyber-misappropriation of trade secrets is increasing.

A number of macro trends indicate that misappropriation of trade secrets, especially cyber-misappropriation will increase. From an economic

---

[102] *See, e.g.*, 5 U.S.C. § 552(b); 75 Fed. Reg. 29754, 29756 (May 27, 2010) (stating the Environmental Protection Agency's interpretation of the Toxic Substances Control Act that chemical identities must be included in health and safety studies made available to the public even if such information is a trade secret).

[103] *See, e.g.*, 5 U.S.C.A. § 2302(b)(8) (West 1996 & Supp. 2006); N.Y. Lab. Law § 740 (West 2002 & Supp. 2006).

[104] Baum v. Jones & Laughlin Supply Co., 233 F.2d 865, 870 (10th Cir. 1956) (holding that after a trade secret is publicly disclosed, there is no trade secret to give rise to a misappropriation claim).

[105] *See* UTSA § 1(4).

[106] *See* UTSA § 1(2); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) ("A trade secret law, however, does not offer protection against discovery by fair and honest means, such as by independent invention. . . .").

perspective, companies rely heavily on increasingly valuable trade secrets for competitive advantage.[107] In an increasingly information-based economy, companies must rely on trade secrets to protect their competitive advantage.[108] This is vividly reflected in the increase in trade secret litigation. Trade secret litigation in federal court appears to have doubled between 1988 and 1995, and again between 1995 and 2004.[109] Trade secret litigation in state courts has also grown at a steady rate.[110] Given the high cost of trade secret litigation,[111] these numbers suggest that trade secrets are increasingly important to companies.

Cyber-misappropriation will likely make up an increasing share of trade secret misappropriation.[112] Not only are trade secrets more accessible through computers, but cyber-misappropriation is also often an easier way to acquire data than through physical means. In the past, physically retrieving, removing, storing, and transferring documents involved a

---

[107] *See generally* David S. Almeling, *Seven Reasons Why Trade Secrets are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1104-1106 (2012) (providing seven reasons that trade secrets have become more important, including the increasing competitive need for trade secrets in a knowledge-based economy); Vincent Chiappetta*, Myth, Chameleon or Intellectual Property Olympian? A Normative Framework Supporting Trade Secret Law*, 8 GEO. MASON L. REV. 69, 71-72 (1999) (noting the "dramatically increased importance of trade secret law in the world of commerce," and that "businesses and their legal advisors clearly believe that trade secret law matters").

[108] *See* Catherine L. Fisk, *Knowledge Work: New Metaphors for the New Economy*, 80 CHI.-KENT L. REV. 839, 857 (2005) ("Virtually every observer from every possible perspective agrees that changes in the economy of industrial and postindustrial nations and the world as a whole have increased the importance of intellectual capital"); David S. Almeling, *Seven Reasons Why Trade Secrets are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1104-1106 (2012); *see generally* Wesley M. Cohen et al., *Protecting Their Intellectual Property Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)* 7 (Nat'l Bureau of Econ. Research, Working Paper No. 7552, 2000), *available at* http://www.nber.org/papers/w7552 (finding that American firms most heavily rely on secrecy to protect product innovations).

[109] *Federal Study*, *supra* note 28, at 293. This study analyzed cases "in which a U.S. district court expressly decided a substantive issue based on trade secret law." *Id.* at 298. As a result, it does not perfectly reflect all trade secret litigation in federal courts or trade secret litigation generally, much of which may result in settlements.

[110] *State Study, supra* note 26, at 68.

[111] Gilson, *supra* note 74, at 599; SHARON SANDEEN & ELIZABETH ROWE, TRADE SECRET LAW IN A NUTSHELL § 4.12.3 (West 2013); American Intellectual Property Law Association, 2013 Report of the Economic Survey (2013), http://www.patentinsurance.com/custdocs/2013AIPLA%20Survey.pdf.

[112] *See* Aaron J. Burstein, *Trade Secrecy as an Instrument of National Security? Rethinking the Foundations of Economic Espionag*e, 41 ARIZ. ST. L.J. 933, 944-46 (2009) (outlining the increasing concern in US government counterintelligence reports about cyber-espionage).

significant logistical challenge.[113] Now, as companies digitize their information, hundreds of thousands of documents can easily be stored on a CD or a flash drive.[114] The information can then be sent anywhere there is internet access at the push of a button. The internet also broadens the field of possible misappropriators.[115] Any computer system linked to the internet is vulnerable to hackers all over the world.[116] Finally, the increase in cloud computing, mobile devices, and employees working from remote locations makes data available from many more points, often across national boundaries.[117]

The Chinese government, and to a lesser degree, the Russian government, encourage and, in some cases, directly participate in the appropriation of other countries' technologies and business information.[118] In the case of China, developing its technological capabilities is a key component of its plan to transform its economy.[119] The latest form of this

---

[113] OFFICE OF THE NATL. COUNTERINTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 2009-2011 2 (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [hereinafter ONCIX 2011].

[114] ONCIX 2011, *supra* note 113, at 2.

[115] *See* ERIC M. DOBRUSIN & RONALD A. KRASNOW, INTELLECTUAL PROPERTY CULTURE: STRATEGIES TO FOSTER SUCCESSFUL PATENT AND TRADE SECRET PRACTICES IN EVERYDAY BUSINESS 234 (2008) ("With [new ideas and the internet] also grew the opportunity for misappropriation of the ideas and the technological means for achieving such misappropriations."); ONCIX 2011, *supra* note 113, at 1-2.

[116] *Id.* at 1-2.

[117] ONCIX 2011, *supra* note 113, at 6-7; Cert 2013 Survey, *supra* note 46, at 1 ("Leaders are unknowingly increasing their digital attack vulnerabilities by adopting social collaboration, expanding the use of mobile devices, moving the storage of information to the cloud, digitizing sensitive information, moving to smart grid technologies, and embracing workforce mobility alternatives. . . ."); *see also* Sharon K. Sandeen, *Lost in the Cloud: The Implications of Cloud Computing for Trade Secret Protection*, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1685402 (Apr. 4, 2012).

[118] ONCIX 2011, *supra* note 113, at 5; THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY, THE IP COMMISSION REPORT 14-19 (May 2013), *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf [hereinafter IP COMMISSION REPORT].

[119] IP COMMISSION REPORT, *supra* note 118, at 7 (technological industries); JAMES MCGREGOR, U.S. CHAMBER OF COMMERCE, CHINA'S DRIVE FOR 'INDIGENOUS INNOVATION'—A WEB OF INDUSTRIAL POLICIES 17 (July 28, 2010), *available at* http://www.uschamber.com/sites/default/files/reports/100728chinareport_0.pdf ("Premier Wen himself in December 2007 urged faster progress on the indigenous innovation program, saying that 'in today's world, science and technology is the ultimate deciding factor of a nation's overall competitiveness, with indigenous innovation acting as the bones to support the rise of a nation.'").

strategy is the "indigenous innovation policy."[120] Ironically, the "indigenous innovation policy" espouses copying innovation from other countries, both openly, for example, by requiring that foreign companies disclose trade secrets as a condition for operating in China,[121] and covertly, through sponsoring the cyber-misappropriation of trade secrets.[122]

Cybersecurity experts had suspected for years that the Chinese government supported hacking into foreign organizations, especially American organizations, to obtain useful confidential information.[123] In February 2013, the security company Mandiant provided the first convincing public evidence that the Chinese government directly sponsors the hacking of American companies to take trade secrets.[124] Mandiant traced 141 cases of cyber-misappropriation—115 in the United States—to one unit of the Chinese People's Liberation Army, Unit 61398.[125] This unit was a substantial enterprise. Mandiant estimated that the work involved over 1,000 servers and dozens—perhaps hundreds—of staff, including linguists, malware authors, industry experts, and IT personnel.[126] As Mandiant stated, "the most probable conclusion is that [this unit] is able to wage such a long-running and extensive cyber espionage campaign because it is acting with the full knowledge and cooperation of the government."[127]

The intrusions identified by Mandiant are not an isolated set of attacks. The Chinese government has likely provided support for many other instances of cyber-misappropriation.[128] Indeed, Verizon estimated that of the 125 cases of confirmed breaches involving trade secret espionage that

---

[120] MCGREGOR, *supra* note 119, at 17.
[121] MCGREGOR, *supra* note 119, at 30.
[122] ONCIX 2011, *supra* note 113, at 5; IP COMMISSION REPORT, *supra* note 118, at 43; MANDIANT APT 1, *supra* note 1, at 2.
[123] *See, e.g.*, U.S.-China Economic and Security Review Commission, 2008 Report to Congress, 110th Cong., 2d Sess. 164 (2008) ("The Chinese government closely monitors Internet activities and is likely aware of the hackers' activities."); ONCIX 2011, *supra* note 113, at 5, 7-8; MCAFEE, REVEALED: OPERATION SHADY RAT 6 (2011), AVAILABLE AT http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf [hereinafter SHADY RAT].
[124] MANDIANT APT 1, *supra* note 1, at 2.
[125] *Id.* at 3, 21.
[126] *Id.* at 5.
[127] *Id.* at 60.
[128] U.S.-China Economic and Security Review Commission, 2012 Report to Congress: Executive Summary and Recommendations, 112th Cong., 2d Sess. 12 (2012), *available at* http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress-Executive%20Summary.pdf.

it collected in 2013, 96 percent were attributable to Chinese state-affiliated actors.[129]

Although Russia has not been linked as directly as China to specific cases of economic cyber-espionage, Russian leaders have explicitly stated that intelligence collection serves the goal of developing Russian science and technology for economic purposes.[130] America arrested Russian spies allegedly tasked with collecting economic and technology information in 2010, and there is evidence to suggest that Russia uses cyber means to collect such information.[131]

International organized crime supplies another group of highly organized and well-financed hackers. The resources and organization of criminal gangs of course pale in comparison to the capabilities of the Chinese or Russian governments. Nevertheless, these criminal gangs are sometimes so large and well organized that they employ hundreds of people, including their own research and development departments.[132] Up to this point, cyber-criminals have focused more on stealing credit card information and personal credentials, but studies find that they are now turning their attention to misappropriating trade secrets, too.[133]

The combination of trade secret holders' reliance on computer systems and the rise of the highly organized attackers just described appear to have combined to produce a dangerous new form of threat in the last few years—the advanced persistent threat (APT). The hackers engaged in APTs

---

[129] VERIZON 2013 REPORT, *supra* note 46, at 11 n.9, 21. Not all hacking by Chinese citizens is necessarily sponsored by the government. China has a widespread culture of hacking including many enterprises that openly provide hacking services. Edward Wong, *Hackers Find China Is Land of Opportunity*, N.Y. TIMES, May 22, 2013, http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html.

[130] ONCIX 2011, *supra* note 113, at 6.

[131] ONCIX 2011, *supra* note 113, at 5, Annex B-2 ("Germany's BfV notes that Russia uses [computer network exploitation] and e-mail interception to save billions of dollars on R&D in the energy, information technology, telecommunications, aerospace, and security sectors.")

[132] MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 15, 19 (Jan. 29, 2009), *available at* http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf [hereinafter MCAFEE UNSECURED ECONOMIES] ("According to Tim Shimeall of Carnegie Mellon University, the biggest source of threat in Russia is its mafia. 'They have immense resources and proved to be ruthless. It is stated that eight percent of the world's deposits is owned by them. With resources like that, the mafia can build its own communication infrastructure.'").

[133] MCAFEE UNSECURED ECONOMIES, *supra* note 132, at 18. This may be particularly in the countries where companies have few scruples about taking proprietary information from competitors. *Id.* at 21.

breach the victims' computer systems and stealthily monitor their activities over the course of months, even years.[134] As a result, these intruders gain continuing access to trade secrets and other confidential information, a window into an organization's secrets.[135] APT attacks are highly sophisticated. They require constant monitoring and stealth from the attacker over a long period of time.[136] In the cases identified by Mandiant, for example, Unit 61398 took trade secrets from organizations over a period of six years. The material it took included technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails, and contact lists.[137]

Statistics in this area can be unreliable because organizations often do not know that they have been compromised.[138] Even when they are aware of the compromise, they may not report it.[139] In addition, the security companies that provide much of the statistics have a business incentive to report alarmingly large numbers on cyber-intrusion.[140] The responses from companies themselves may be misleading because respondents may not know the precise definition of a trade secret. They may report that any information breached is a "trade secret." Nevertheless, the available statistics suggest that the numbers are significant and increasing. For example, Verizon reported 120 cases of cyber-misappropriation in 2012.[141] In 2011, the Poneman Institute reported that the companies it surveyed experienced a stunning 1.4 successful attacks per company a week, and a 44

[134] SHADY RAT, *supra* note 123, at 2.
[135] *Id.*
[136] *Id.*
[137] MANDIANT APT 1, *supra* note 1, at 3. McAfee revealed another APT, which hacked and monitored 71 organizations for months and years. SHADY RAT, *supra* note 123, at 4, 9.
[138] VERIZON 2013 REPORT, *supra* note 46, at 10; SHADY RAT, *supra* note 123, at 1.
[139] VERIZON 2013 REPORT, *supra* note 46, at 10; ONCIX 2011, *supra* note 113, at i. Even where reporting is required, organizations do not always comply. For example, cleared defense contractors are required by law to file reports of suspicious contacts indicative of foreign threats. Defense Security Service, Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reports 10 (2013), *available at* http://www.dss.mil/documents/ci/2013%20Unclass%20Targeting%20US%20Technologies_FINAL.pdf. Only about ten percent of them, however, provide any sort of reporting. ONCIX 2011, *supra* note 113, at A-1.
[140] *See* Peter Maass & Megha Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, *ProPublica*, Aug. 1, 2012, http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion (noting the observation of a cyber-security expert that security companies "have a vested interest in portraying a more dangerous environment because they stand to gain for it").
[141] VERIZON 2013 REPORT, *supra* note 46, at 11 n.9, 18 fig. 8.

percent increase in cyber-attacks over the previous year.[142] In another study, a full third of companies surveyed reported more cyber-attacks in 2013 than in 2012.[143]

B. The Protectionist Response to the Cyber-Misappropriation Threat

In response to the threat of cyber-misappropriation, trade secret holders and leaders across the political spectrum have pushed for more trade secret protections. Congress has already enacted several statutes bolstering protection. More federal legislation seems likely. Indeed, the media attention and florid rhetoric surrounding cyber-misappropriation may be creating the momentum for radical change to trade secret law. In particular, it seems increasingly probable that trade secrets will join the other major branches of intellectual property by gaining a private cause of action under federal law. Such a sweeping law has the potential to remake trade secret law, which has, up to this point, been governed chiefly by state law. If trade secret law were federalized by simply adding a private right of action to the Economic Espionage Act, as many have proposed, the new law would dramatically strengthen trade secret law in this country.

1. The One-Sided and Inaccurate Rhetoric on Trade Secret Cyber-Misappropriation

Politicians on both sides of the aisle have quickly recognized the political advantages of presenting themselves as tough on cyber-theft of trade secrets. The issue of cyber-misappropriation offers a potent mix of nationalism, property rights, moral outrage, and concerns about job security in already depressed economic times. The result has been one-sided, alarmist and often inaccurate rhetoric on the subject. The danger is that this rhetoric will lead to one-sided legislation that favors trade secret holders' interests over all other interests.

Apparently to emphasize the seriousness of the issue, political leaders have exaggerated the threat or relied on stunningly large but unverified numbers about the damage caused by cyber-hacking. Perhaps the

---

[142] PONEMON STUDY, *supra* note 2, at 1. These attacks included cyber-attacks other than cyber-misappropriation. *Id.* Cisco System's report in 2011 shows similar numbers. Cisco Systems found a 46 percent increase in web malware during the first quarter of 2011 alone. CISCO SYSTEMS, CISCO 1Q11 GLOBAL THREAT REPORT 2 (2011), *available at* http://www.cisco.com/web/about/security/intelligence/reports/cisco_global_threat_report_1Q2011.pdf.

[143] CERT 2013 SURVEY, *supra* note 46, at 14.

best example of this exaggeration is the statement by the Director of the National Security Agency that cyberhacking has led to "the greatest transfer of wealth in history."[144] Members of Congress and the press have repeated General Alexander's phrase *ad nauseam* and without question.[145] Nevertheless, the statement is absurd. One need only think of colonialism—the exploitation of most of the world by a few countries—to imagine a greater transfer of wealth.[146]

Public rhetoric on the subject also regularly employs eye-popping numbers on the level of cyber-hacking damage. General Alexander has claimed at different points that intellectual property theft costs Americans $250 billion or $300 billion per year.[147] President Obama stated in a speech that cyber-criminals steal $1 trillion worth of intellectual property

[144] Gen. Keith B. Alexander, Director, National Security Agency, Keynote Address at American Enterprise Institute: Cybersecurity and American Power (July 9, 2012), *available at* http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/.

[145] *See, e.g.*, Members of Congress: 159 CONG. REC. S3165-66 (daily ed. May 7, 2013) (statement of Sen. Carl Levin); *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology: Hearing Before the H. Subcommittee on Oversight and Investigations,* 113th Cong. (July 9, 2013) (statement of Rep. Tim Murphy), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/OI/20130709/HHRG-113-IF02-MState-M001151-20130709.pdf.
Media: Emil Protalinski, *NSA: Cybercrime is "the greatest transfer of wealth in history"*, ZDNET, July 10, 2012, *available at* http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598/; Chris Strohm & Nicole Gaouette, *U.S. Downplays Spying Accusations in China Hacking Talks*, BLOOMBERG NEWS, July 8, 2013, *available at* http://www.bloomberg.com/news/2013-07-08/spying-accusations-shadow-u-s-china-cybersecurity-talks.html; Deborah Charles, *Senators Propose Law to Combat Cyber Theft*, NBC NEWS, May 7, 2013, *available at* http://www.nbcnews.com/id/51809261/ns/technology_and_science-security/t/senators-propose-law-combat-cyber-theft/.

[146] Spain alone transferred at least $20 billion of gold and silver in today's dollars from the Americas to Spain before 1600. *See* Murdo J. Macleod, *Spain and America: The Atlantic Trade, 1492-1720*, *in* 1 THE CAMBRIDGE HISTORY OF LATIN AMERICA 341, 358-59, 365 (Leslie Bethell ed., 1984). This calculation is based on estimates that Spain transferred at least 65 tons of gold and 25,000 tons of silver before 1600. *See id.* These numbers do not take into account the value of dyes, leathers, and other products, not to mention the transfers of valuable minerals in all the centuries following 1600. *See id.* at 358-67.

[147] Jim Garamone, *Cybercom Chief Details Cyberspace Defense*, AMERICAN FORCES PRESS SERVICE, Sep. 23, 2010, *available at* http://www.defense.gov/news/newsarticle.aspx?id=60987 ($300 billion); Gen. Keith B. Alexander, Director, National Security Agency, Keynote Address at American Enterprise Institute: Cybersecurity and American Power (July 9, 2012), *available at* http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/ ($250 billion).

annually.[148] Members of Congress have repeated the $300 billion number many times, variously attributing it to intellectual property theft generally or to trade secret theft specifically.[149]

In reality, there is little to no basis for these numbers.[150] The $300 billion number has been attributed to a report by ASIS International, but no ASIS International report appears to provide that number.[151] The $300 billion estimate may result from rounding up the $250 billion estimate of intellectual property losses annually for U.S. companies in the 1997 ASIS report.[152] Alternatively, it may result from a miscalculation of numbers in

---

[148] Pres. Barack Obama, Remarks by the President on Securing Our Nation's Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

[149] *See, e.g.*, Ryan Davis, *China Worries Improve Prospects Of Trade Secrets Bill*, LAW 360 July 2, 2013, *available at* http://www.law360.com/articles/454818/china-worries-improve-prospects-of-trade-secrets-bill (intellectual property); *Chinese Telecommunications Investigation Open Hearing Before the H. Permanent Select Comm. on Intelligence*, 112th Cong. (Sept. 13, 2012) (statement of Rep. Dutch Ruppersberger), *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/09122012DutchOpening.pdf (trade secrets); *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology Before the H. Subcommittee on Oversight and Investigations,* 113th Cong. (July 9, 2013) (statement of Rep. Tim Murphy), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/OI/20130709/HHRG-113-IF02-MState-M001151-20130709.pdf (intellectual property); *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology Before the H. Subcommittee on Oversight and Investigations,* 113th Cong. (July 9, 2013) (statement of Rep. Fred Upton), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/OI/20130709/HHRG-113-IF02-MState-U000031-20130709.pdf (intellectual property).

[150] For a full discussion of the problems with these statistics, see Peter Maass and Megha Rajagopalan*, Does Cybercrime Really Cost $1 Trillion?*, *ProPublica*, Aug. 1, 2012, *available at* http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion (noting the observation of a cyber-security expert that security companies "have a vested interest in portraying a more dangerous environment because they stand to gain for it.")

[151] For examples of other reports attributing the $300 billion estimation to an ASIS International report, *see* Ruth M. Corbin, *Managing Risk and Protecting Intellectual Property*, IVEY BUSINESS JOURNAL, January/February 2002, *available at* http://iveybusinessjournal.com/topics/the-organization/managing-risk-and-protecting-intellectual-property; OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2002, 1-2 (2002), *available at* http://www.ncix.gov/publications/reports/fecie_all/fecie_2002.pdf. Despite a review of the ASIS International reports and the help of information specialists at ASIS International's O.P. Norton Information Resources Center, the author could not find an ASIS International report that expressly contained the $300 billion estimate.

[152] *See, e.g.*, ASIS INTERNATIONAL, 1997 TRENDS IN INTELLECTUAL PROPERTY LOSS SURVEY REPORT 2 (1998).

the 1998 ASIS report.[153] ASIS reports, however, like many other reports on this subject, themselves admit that estimations on intellectual property loss are unreliable, and have refrained from calculating new estimates in later reports.[154] As a chief economist at the Government Accountability Office's Applied Research and Methods division stated, "we don't find any basis for believing [$300 billion] to be an accurate number."[155]

The truth is that calculating losses from the trade secret theft is very difficult.[156] A number of researchers have attempted to do so, and have produced wildly differing estimations.[157] One of the problems is that there is no clear market value for a given trade secret.[158] The reason for this is

---

[153] ASIS calculated that Fortune 1000 companies lost $45 billion worth of proprietary information in a 17-month period. ASIS INTERNATIONAL, 1998 TRENDS IN INTELLECTUAL PROPERTY LOSS SURVEY REPORT 29 (1999). Forty-five billion dollars in losses over a 17-month period would equate to about $32 billion in losses on an annual basis. The 1998 ASIS report stated that it had a 10 percent response rate, so multiplying $32 billion by ten would produce a number close to $300 billion. *Id.* However, the $45 billion estimate was already produced by extrapolating the response rate across the rest of the Fortune 1000. *Id.* at 25. As a result, multiplying $32 billion by ten is a miscalculation by an order of magnitude.

[154] *See, e.g.*, ASIS FOUNDATION, TRENDS IN PROPRIETARY INFORMATION LOSS 26 (2002); ASIS INTERNATIONAL, TRENDS IN PROPRIETARY INFORMATION LOSS 3 (June 2007), *available at* https://www.asisonline.org/ASIS-Store/Products/Pages/Trends-in-Proprietary-Information-Loss.aspx [hereinafter ASIS 2007 SURVEY]; IP COMMISSION REPORT, *supra* note 118, at 23; CERT 2013 SURVEY, *supra* note 46, at 3.

[155] Natasha Dhillon, *Witnesses, Lawmakers at House Hearing On IP Theft, Cyber Espionage Take Aim at China, BNA Snapshot*, BUREAU OF NATIONAL AFFAIRS, July 9, 2013.

[156] IP COMMISSION REPORT, *supra* note 118, at 23; JAMES ANDREW LEWIS & STEWART BAKER, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE 16 (July 2013), *available at* http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage [hereinafter CSIS REPORT] ("[A] precise single figure for the cost of cyber crime and cyber espionage is unattainable . . . ."); OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2003 2 (2003), *available at* http://www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf ("The Counterintelligence (CI) Community cannot accurately establish the dollar cost to the nation of the loss of trade secrets, but we believe the flow has eroded the US global military and economic advantage.").

[157] Estimates from academic literature on the losses from economic espionage range so widely as to be meaningless—from $2 billion to $400 billion or more a year—reflecting the scarcity of data and the variety of methods used to calculate losses. *See* ONCIX 2011, *supra* note 113, at 4; CSIS REPORT, *supra* note 156, at 6.

[158] Even the market value fails to indicate the amount of the loss because the infringer likely would not have purchased the information if it were available for sale. Moohr, *supra* note 53, at 900-01 ("The estimates of lost value are often based on an assumption that infringers would have purchased the object if it was not otherwise available, and there is no

simple: trade secrets are secret and not sold on an open market.[159] Without a readily identifiable market value, researchers are often thrown back on the biased estimates of the companies themselves.[160]

Of course, the fact that the amount of harm caused by cyber-misappropriation is hard to ascertain does not prove that the threat is negligible. As discussed in Part II.A, *infra*, there are many reasons to be worried about cyber-misappropriation. But politicians' willingness to espouse these unverifiable numbers indicates their interest in provoking public concern—and likely their hope to reap the political benefits of taking action on trade secret theft.

Moreover, politicians' acceptance of these numbers suggests a basic misconception about trade secrets—or at least a readiness to engage in misleading rhetoric on the subject. The misconception is that the taking of a trade secret results in an absolute loss of that information to the trade secret holder. The reality is more complicated. President Obama's claim in a speech that a "single employee of an American company was convicted of stealing intellectual property reportedly worth $400 million" illustrates the problem.[161] The statement implies that the company suffered $400 million in losses. In fact, this particular company, DuPont, apparently lost nothing. The government prosecutors admitted that there was no evidence that any of the information that the employee had copied was transferred to a third party.[162]

But even if the employee had conveyed DuPont's trade secrets to a competitor, it is highly unlikely that the damages to DuPont would amount to $400 million. As discussed above, the market for trade secrets is difficult to determine. Trade secret losses are hard to calculate for another basic reason. Because trade secrets are information, they are typically not stolen in the sense that the thief obtains the item and the victim loses it. Instead, as

---

evidence that this is the case."); *State Study*, *supra* note 26, at 292 ("There is little data on the exact value of trade secrets because trade secrets are, by definition, secret.").

[159] *State Study*, *supra* note 26, at 292.

[160] For example, in United States v. Min, DuPont valued the trade secrets taken by the defendant at $400 million. Memorandum of Plea Agreement at 2, United States v. Min, No. 1:06-cr-00121-SLR (D. Del. Nov. 13, 2006). However, DuPont did not suffer $400 million in damages. *See* Government's Response to Defendant's Motion for Downward Departure at 7-8, United States v. Min, No. 1:06-cr-00121-SLR (D. Del. Nov. 5, 2007).

[161] Pres. Barack Obama, Remarks by the President on Securing Our Nation's Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

[162] Government's Response to Defendant's Motion for Downward Departure at 7-8, United States v. Min, No. 1:06-cr-00121-SLR (D. Del. Nov. 5, 2007).

in the DuPont case, trade secret misappropriators copy the information.[163] Thus, the loss to the trade secret holder is not the loss of the information; it is instead the loss of the competitive advantage the information provided with regard to the party that obtained the information.[164] Depending on how well the new possessor takes advantage of that information and how directly it competes with the initial trade secret holder, the victim may suffer heavy losses, or none at all.[165] Where the victim does not know the identity of the misappropriator, as is often the case in cyber-misappropriation, the loss can be almost impossible to determine with accuracy.[166]

The language of the debate on trade secrets not only simplifies and exaggerates damages, it conflates the taking of trade secrets with "theft," "stealing," and "robbery," appropriating the emotional and moral connotations of these terms.[167] For example, Senator Carl Levin fumed, "[i]t is outrageous that American trade secrets are being stolen,"[168] and Representative Mike Rogers stated dramatically that China is "robbing U.S. ingenuity and innovation."[169] But, as the Supreme Court observed, interference with intellectual property "does not easily equate to theft."[170]

---

[163] Government's Response to Defendant's Motion for Downward Departure at 4-5, United States v. Min, No. 1:06-cr-00121-SLR (D. Del. Nov. 5, 2007).

[164] UNIF. TRADE SECRETS ACT § 3; Moohr, *supra* note 53, at 918; *see generally* CSIS REPORT, *supra* note 156.

[165] *See* UNIF. TRADE SECRETS ACT § 3; *see, e.g.*, University Computing Co. v. Likes-Youngstown Corp., 504 F.2d 518, 536 (5th Cir. 1974) (identifying the plaintiff's lost profits and the "benefits, profits, and advantages gained by the defendant in the use of the trade secret" as potential measure of damages); In re Jonatzke, 47 B.R. 846 (Bkrtcy. E.D. Mich. 2012) (identifying lost profits, erosion of market share, and out-of-pocket expenses as possible measures of damages).

[166] IP COMMISSION REPORT, *supra* note 118, at 40. For a discussion of how difficult it can be to estimate losses due to another kind of intellectual property rights infringement—copyright infringement—see Julian Sanchez, *750,000 Lost Jobs? The Dodgy Digits Behind the War on Piracy*, ARS TECHNICA, Oct. 7, 2008, *available at* http://arstechnica.com/tech-policy/news/2008/10/dodgy-digits-behind-the-war-on-piracy.

[167] *See, e.g.*, Eamon Javers, *White House Mobilizes to Stop Theft of Trade Secrets*, CNBC, (Feb. 21, 2013, 3:55 PM), *available at* http://www.cnbc.com/id/100481542 ("The Obama administration is mobilizing the full force of the federal government in an effort to stop theft of trade secrets from American companies.").

[168] 159 CONG. REC. S3165-66 (daily ed. May 7, 2013) (statement of Sen. Carl Levin).

[169] Press Release, U.S Senate Committee on Homeland Security & Governmental Affairs, Financial & Contracting Oversight Subcommittee, Bipartisan Effort to Punish Nation-State Cyber Hackers (June 6, 2013), *available at* http://www.hsgac.senate.gov/subcommittees/fco/media/ranking-member-johnson-joins-bipartisan-effort-to-punish-nation-state-cyber-hackers.

[170] Dowling v. United States, 473 U.S. 207, 216-17 (1985). The Supreme Court was discussing copyright, but the same observations apply to trade secrets. *See id.* A trade

The simple binary formulation in personal property law that any unauthorized taking is a theft and therefore morally wrongful does not apply in trade secret law. Instead, trade secret law countenances many ways in which trade secrets may be acquired without authorization—reverse engineering, accidental disclosure, and so on—because the dissemination of useful information serves the public interest.[171] Referring to trade secret misappropriation as theft simplifies misappropriation into black and white moral terms. Those who take information held by another become "thieves," regardless of whether the information meets the specific criteria of a trade secret or qualifies as misappropriation.[172] This rhetoric no doubt appeals to deeply rooted American notions on the sanctity of property, but it does not accurately reflect the risks to trade secrets.[173]

Of course, no one expects politicians to discuss legal issues with perfect precision. But the rhetoric displays a one-sided focus on information holder's interests, according them an apparently unlimited right to information as their property. This language disregards the policy concerns favoring public access to information. More fundamentally, it discounts the basic rationale underlying trade secret law: trade secret rights are intended to serve the public interest, not trade secret holders specifically.[174]

Public discussion of cyber-misappropriation also plays on the public's fears by linking the issue to job loss and threats to national security. Again, these concerns are real, but they present a one-sided and emotional picture of the cyber-misappropriation problem.

Political leaders emphasize repeatedly that trade secret theft threatens American jobs. Senator John McCain, for example, stated that cyber-espionage "kills American jobs."[175] In this area too, the rhetoric relies on massive, unverified numbers, such as Congressman Tim Murphy's claim that the theft of intellectual property "translates into roughly 2.1 million lost

---

secret also "comprises . . . [a] delimited interest[] to which the [common] law affords correspondingly exact protections." *See id.* at 216.

[171] *See supra* notes 78-81 and accompanying text.

[172] *See, e.g.*, 159 CONG. REC. S3165-66 (daily ed. May 7, 2013) (statement of Sen. Carl Levin).

[173] *See, e.g.*, JENNIFER NEDELSKY, PRIVATE PROPERTY AND THE LIMITS OF AMERICAN CONSTITUTIONALISM 4 (University of Chicago Press, 1990) (arguing that a concern with private property rights shapes American institutions, its political system, and its conception of limited government).

[174] *See supra* Part I.B.

[175] Press Release, Office of U.S. Senator Carl Levin, Bipartisan Group of Senators Introduces Legislation to Combat Cyber Theft (May 7, 2013), *available at* http://www.levin.senate.gov/newsroom/press/release/bipartisan-group-of-senators-introduces-legislation-to-combat-cyber-theft.

jobs."[176] As a recent report observed, such numbers are highly uncertain.[177] Nevertheless, threats to jobs are an emotionally resonant issue for the public, especially in the current economy of persistently high unemployment.[178]

Finally, the rhetoric tends to subsume risks to trade secrets into risks to national security.[179] Some trade secrets directly implicate national security, such as secrets related to military contractors. Political leaders have tended to emphasize this connection by highlighting instances in which cyber-hackers have taken information about military technology from defense contractors.[180] But cyber-crime losses inflicted on defense contractors appear to comprise only a fraction of cyber-crime losses overall.[181]

Members of Congress and the Obama Administration have not just linked the limited instances of trade secret misappropriation from defense contractors to national security concerns. They have conflated economic

---

[176] *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology Before the H. Subcomm. on Oversight and Investigations,* 113th Cong. (July 9, 2013) (statement of Tim Murphy, H. Rep.), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/OI/20130709/HHRG-113-IF02-MState-M001151-20130709.pdf.

[177] CSIS REPORT, *supra* note 156, at 17.

[178] *See* Labor Force Statistics from the Current Population Survey, *Databases, Tables & Calculators By Subject,* U.S. BUREAU OF LABOR STATISTICS (data extracted Nov. 13, 2013), http://data.bls.gov/timeseries/LNS14000000

[179] For example, Senator Ron Johnson declared: "Theft of U.S. intellectual property . . . costs American jobs, innovation, and threatens national security." Press Release, U.S. Senate Comm. on Homeland Sec. & Governmental Affairs, Fin. & Contracting Oversight Subcomm., Bipartisan Effort to Punish Nation-State Cyber Hackers (June 6, 2013), *available at* http://www.hsgac.senate.gov/subcommittees/fco/media/ranking-member-johnson-joins-bipartisan-effort-to-punish-nation-state-cyber-hackers; *see also* Fahmida Y. Rashid, *U.S. Senators Introduce 'Deter Cyber Theft Act' to Help Protect Trade Secrets*, SECURITYWEEK, May 9, 2013, *available at* http://www.securityweek.com/us-senators-introduce-deter-cyber-theft-act-help-protect-trade-secrets; Press Release, Office of U.S. Senator Carl Levin, Bipartisan Group of Senators Introduces Legislation to Combat Cyber Theft (May 7, 2013), *available at* http://www.levin.senate.gov/newsroom/press/release/bipartisan-group-of-senators-introduces-legislation-to-combat-cyber-theft (Cyber-espionage "kills American jobs, undermines the competitiveness of our businesses and compromises U.S. economic and national security interests, and it must stop now.").

[180] For example, in introducing the Deter Cyber Theft Act, Senator Levin gave the example of cyber-espionage against QinetiQ, a defense contractor, that "jeopardized the [victim] company's sensitive technology involving drones, satellites, the U.S. Army's combat helicopter fleet, and military robotics." 159 CONG. REC. S3165-66 (daily ed. May 7, 2013) (statement of Sen. Carl Levin).

[181] PONEMON STUDY, *supra* note 2, at 11.

harm caused by taking any business secret with harm to national security.[182] The House Report on the Cyber Intelligence Sharing and Protection Act illustrates the conflation of economic and national security risks:

> Perhaps most troubling, these [efforts by advanced nation-state actors to penetrate American computer systems and networks] are targeted not only at sensitive national security and infrastructure information, but are also often aimed at stealing the corporate research and development information that forms the very lifeblood of the American economy. . . . There can be no question that in today's modern world, economic security is national security. . . .[183]

This reasoning makes little sense from a policy perspective. First, it disregards any meaningful limit on national security risks. If economic loss is the measure of a national security risk, traffic congestion is a national security risk.[184]

Second, the policy goals in the two areas are in tension with each other.[185] Trade secret law protects information as a means for providing incentives to invent and to exchange information.[186] In contrast, the goal of protecting information for national security reasons is to prevent disclosures that would harm national interests.[187] As a result, trade secret holders and the government will not always act in ways that serve each other's interests. For example, trade secret misappropriation by a foreign actor has no effect on a trade secret holder's economic interest if that actor does not compete in the same market. As a result, a trade secret holder may not enforce its rights against the foreign actor even if the loss of the trade secret harms national

---

[182] H. REP. NO. 113-039 at 9 (2013). This reasoning goes back at least to the passage of the EEA when the House Report stated: "There can be no question that the development of proprietary economic information is an integral part of America's economic well-being. Moreover, the nation's economic interests are a part of its national security interests. Thus, threats to the nation's economic interest are threats to the nation's vital security interests." H.R. Rep. No. 104-788, *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023.

[183] H.R. Rep. No. 104-788, *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023.

[184] Burstein, *supra* note 112, at 947.

[185] *See id.* at 963-68.

[186] *See, e.g.*, Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178 (7th Cir. 1991). The other chief rationale for trade secret law—enforcing standards of commercial morality—is also in tension with national security concerns. *See* Burstein, *supra* note 112, at 966-69.

[187] Burstein, *supra* note 112, at 965.

security.[188] Conversely, from a national security perspective, trade secret misappropriation among American companies is not worth pursuing, because it causes little harm to national interests.

Thus, it seems that the principal benefit from classifying trade secret cyber-misappropriation as a national security threat is to increase the public sense of urgency with respect to protecting trade secrets. Stronger trade secret protections will seem imperative if risks to trade secrets threaten our national security.

It is unclear whether politicians act from ignorance or political expediency in disregarding countervailing policy concerns. Ignorance may be the reason. Compared to other areas of intellectual property law, trade secrets have received little attention on a federal level. Trade secrets, unlike patent, copyright, and trademark, are primarily governed by state law, not federal law.[189] From a common familiarity point of view, politicians, like the public, may be less familiar with trade secret information simply because such information is secret. In contrast, the average person encounters material protected by copyright, trademark, or patent law on a daily basis.[190] In any case, it may not matter why members of Congress and the Obama administration discuss trade secret law in one-sided terms based on lack of knowledge or political opportunism. Whatever the reason, the result is that they promote policies heavily weighted toward trade secret holders' rights.

2. Strengthening Trade Secret Rights through Federal Law

The combination of cyber-risks and protectionism may lead to a radical strengthening of trade secret law. Congress has already enacted statutes increasing trade secret protection under criminal law. The logical next step is to strengthen civil trade secret law through a federal law. A federal civil trade secret law could provide advantages over the current state

---

[188] As the ONCIX 2011 report observed, U.S. private industry representatives cared little about whether their information was collected by foreign intelligence services or by criminals, although collection by the former has greater impact on national security. ONCIX 2011, *supra* note 113, at 1-2.

[189] *See supra* Part I.A. and *infra* note 205 and accompanying text. Although Congress passed the EEA, it has not been a high profile law. Since its passage in 1996, there have been only around one hundred indictments and a handful of convictions. Peter J. Toren, *An Analysis of Economic Espionage Act Prosecutions: What Companies Can Learn From It and What the Government Should Be Doing About It!*, 84 BNA PATENT, TRADEMARK, & COPYRIGHT J. 884, 2 (2012).

[190] An average American citizen listens to copyright-protected music or sees a trademark every day. To a lesser extent, Americans may be familiar with the label "patented" or "patent pending" on ordinary products.

system, but it need not grant stronger rights to trade secret holders than state law to provide the advantages of federalization. Nevertheless, due to Congress's one-sided concern with protecting trade secrets, any federal civil trade secret law enacted now is likely to grant much stronger rights to trade secret holders than existing state law.

In 2012, Congress upped the penalties for violating the EEA and broadened its reach to apply to a broader range of interstate activity.[191] More legislation appears likely. The Obama administration is now conducting a legislative review to determine if additional legislation is needed to enhance enforcement against trade secret theft.[192] Meanwhile, a number of bills have been proposed or are now pending in Congress to provide additional protection to trade secret holders.[193]

One obvious legislative change would be to create a private party cause of action for trade secret misappropriation under federal law. Some commentators on trade secret law have advocated a federal civil trade secret law for years.[194] Now, however, due to concerns about cybersecurity,

---

[191] The Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236 (codified at 18 U.S.C. § 1832(a) (2013)); The Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269 (codified at 18 U.S.C. §§ 1831(a)-(b) (2013)).

[192] OFFICE OF THE PRESIDENT OF THE UNITED STATES, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 12 (Feb. 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [hereinafter ADMINISTRATION STRATEGY].

[193] Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014); Future of American Innovation and Research Act of 2013, S. 1770, 113th Cong. (2013); Private Right of Action Against Theft of Trade Secrets Act of 2013, H.R. 2466, 113th Cong. (2013); Protecting American Trade Secrets and Innovation Act of 2012, S. 3389, 112th Cong. (2012); Cyber Economic Espionage Accountability Act, S. 1111, 113th Cong. (2013); Cyber Economic Espionage Accountability Act, H.R. 2281, 113th Cong. (2013); Deter Cyber Theft Act, S. 884, 113th Cong. (2013).

[194] *See* Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427 (1995); Moohr, *supra* note 53, at 920; R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656, 668 (2008) (proposing amending the EEA to add a private civil cause of action without preempting state law); *see* David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769, 773 (2009) [hereinafter *Four Reasons*]; Lao, *supra* note 23, at 1667. No commentator appears to offer a robust defense of the state law system. The American Intellectual Property Law Association wrote a report in 2004 concluding that the benefits of a federal civil trade secret were outweighed by the costs: the additional burden on federal courts and the loss of state control over the regulation of their economies. Report of the Trade Secrets Committee, American Intellectual Property Law Association, (2004), *available at* http://www.aipla.org/committees/committee_pages/Trade_Secret_Law/Pages/default.aspx. However, the AIPLA appears to have changed its mind, at least in part, because it

advocacy for federalizing trade secret law has intensified. Four bills in Congress propose federalizing civil trade secret law.[195] And more than half of the parties that responded to the Obama administration's request for public comments on legislation to combat foreign trade secret theft specifically recommended a federal civil trade secret law.[196] More recently, the IP Commission, a bipartisan commission on the theft of American intellectual property, advocated a federal civil trade secret law in May 2013.[197]

---

recommended a private party cause of action against foreign misappropriation under federal law to IPEC. *See* Jeffrey Lewis, Response to Request for Public Comments for "Trade Secret Theft Strategy Legislative Review" (78 Fed. Reg. 16875, March 19, 2013), AIPLA, Apr. 22, 2013, *available at* http://www.aipla.org/committees/committee_pages/Trade_Secret_Law/Committee%20Documents/4.%20AIPLA%20Letter%20to%20IPEC%20on%20Trade%20Secrets%204-22-2013.pdf.

[195] Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014); Future of American Innovation and Research Act of 2013, S. 1770, 113th Cong. (2013); Private Right of Action Against Theft of Trade Secrets Act of 2013, H.R. 2466, 113th Cong. (2013); Protecting American Trade Secrets and Innovation Act of 2012, S. 3389, 112th Cong. (2012).

[196] IPEC specifically invited "the public to submit recommendations for legislative changes to enhance enforcement against, or reduce the risk of, trade secret theft for the benefit of foreign companies or foreign governments." U.S. Intellectual Property Enforcement Coordinator Request for Public Comments, Docket ID: OMB-2013-0002, FR Doc. 2013-06226, filed Mar. 18, 2013, *available at* http://www.regulations.gov/#!documentDetail;D=OMB-2013-0002-0001. Parties calling for a general federal civil cause of action included the Intellectual Property Owner's Association and the Alliance for Clean Technology Innovation. Intellectual Property Owner's Association, Request for Public Comments on "Trade Secret Theft Strategy Legislative Review" 78 Fed. Reg. 16875 (Mar. 19, 2013), at 1, Apr. 22, 2013, *available at* http://www.regulations.gov/#!documentDetail;D=OMB-2013-0002-0001; Alliance for Clean Technology Innovation, Response to the Request of the U.S. Intellectual Property Enforcement Coordinator for Public Comments: Legislative Review Related to Enforcement Against Economic Espionage and Trade Secret Theft, at 8, Apr. 22, 2013, *available at* http://www.regulations.gov/#!documentDetail;D=OMB-2013-0002-0001. Others, including the American Intellectual Property Law Association and Intel Corporation called for a private party cause of action under federal law only against foreign trade secret misappropriation. *See* Jeffrey Lewis, Response to Request for Public Comments for "Trade Secret Theft Strategy Legislative Review" (78 Fed. Reg. 16875, Mar. 19, 2013), AIPLA, at 2, Apr. 22, 2013, *available at* http://www.aipla.org/committees/committee_pages/Trade_Secret_Law/Committee%20Documents/4.%20AIPLA%20Letter%20to%20IPEC%20on%20Trade%20Secrets%204-22-2013.pdf.
Intel Corp., IPEC Request for Comments on Trade Secret Theft Strategy Legislative Review, at Pt. III, Apr. 22, 2013, *available at* http://www.regulations.gov/#!documentDetail;D=OMB-2013-0002-0001.

[197] IP COMMISSION REPORT, *supra* note 118, at 5.

Trade secret law is now the only one of the four major branches of intellectual property law lacking a federal private party cause of action.[198] Congress could do so under its Commerce Clause power, in the same way that the federal trademark law and the EEA are enacted under Congress's power to regulate interstate commerce.[199]

Ever since the UTSA was adopted, there has been a law review article written every decade or so that advocates for a civil cause of action under federal law.[200] The EEA has not satisfied this demand, since it is only a criminal federal trade secret law.[201] A civil federal trade secret law, according to advocates, could decrease both transactional and enforcement costs for many trade secret holders by improving uniformity in trade secret law across the country.[202]

Although all but two states have adopted the Uniform Trade Secrets Act (UTSA) in some form,[203] almost every state has adopted a slightly different version.[204] As a result, supporters of a civil federal trade secret law

---

[198] *Four Reasons*, *supra* note 194, at 771.

[199] *See* U.S. CONST. art. I, § 8, cl. 3; 15 U.S.C.A. § 1127 ("'commerce' means all commerce which may lawfully be regulated by Congress"); 18 U.S.C. § 1832(a) (limiting protection to trade secrets "used in or intended for use in interstate or foreign commerce").

[200] For more complete discussions of the arguments in favor, *see generally* Almeling, *Four Reasons*, *supra* note 194; Lao, *supra* note 23; Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427 (1995).

[201] With the exception of the provision for civil claims by the Attorney General, 18 U.S.C. § 1836(a). The Computer Fraud and Abuse Act (CFAA), which provides both criminal and civil remedies, may be a stronger contender as a federal trade secret law. Courts have interpreted the CFAA to create liability for the cyber-misappropriation of trade secrets. *See, e.g.*, Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000); George S. May Int'l Co. v. Hostetler, No. 04 C 1606, 2004 U.S. Dist. LEXIS 9740, at *10 (N.D. Ill. May 28, 2004) (finding that infringement of copyrighted material taken from a computer qualifies as impairment of integrity of data under the CFAA). Courts, however, have split on this point. Some courts have held that misappropriation of trade secrets alone fails to satisfy the damage and loss provisions of the CFAA. *See* Consulting Prof'l Res., Inc. v. Concise Techs., LLC, No. 09-1201, 2010 U.S. Dist. LEXIS 32573, at *22 (concluding that a "compromise or decrease in the competitive value of . . . confidential information does not satisfy the [CFAA's] damage requirement"); *see also* Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *26 (M.D. Fla. Aug. 1, 2006) (holding that taking confidential information is not damage under the CFAA).

[202] *See Four Reasons*, *supra* note 194, at 770; Lao, *supra* note 23, at 1636; Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427, 442 (1995).

[203] *See* Lao, *supra* note 23.

[204] States vary on what constitutes misappropriation, the definition of a trade secret, the length of injunctions, exemplary damages, attorney fees, and the statute of limitations. Lao, *supra* note 23, at 1661-65; *see also* Linda B. Samuels & Bryan K. Johnson, *The Uniform*

argue that companies that operate across state lines must invest time and money to investigate the different rules in each state in which it operates.[205] They contend that enforcement costs are higher, too, because of the time involved in researching the specific laws of each state in which the misappropriation occurred and litigating choice-of-law issues.[206] They conclude that a uniform federal law would decrease these costs.[207]

This argument may be overstated. Although the statutes differ in some details, state courts typically agree on the core principles of trade secret law.[208] To the extent that trade secret law varies between states, however, growth in cyber-misappropriation bolsters the argument for a federal civil trade secret law. Due to the fact that cyber-hackers may misappropriate data from wherever they have internet access, the defendants

---

Trade Secrets Act: The States' Response, 24 CREIGHTON L. REV. 49, 51 52 (1990); *Four Reasons*, *supra* note 194, at 779-82. For example, by setting a high standard for misappropriation, Alabama's trade secret law provides considerably less trade secret protection than the UTSA. *See* Long, *The Alabama Trade Secrets Act*, 18 CUMB. L. REV. 557, 567 (1988). Under the Alabama statute, misappropriation requires that the defendant take the trade secret embodied in physical form with intent to use the trade secret in a trade or business. Ala. Code § 8-27-2(1) (1993); Lao, *supra* note 23, at 1662, 1678. The UTSA's definition of misappropriation requires neither that the trade secret be embodied in physical form nor that the defendant intend to use the trade secret in a trade or business. *See* UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 433, 438 (1985). Conversely, North Carolina version of the UTSA sets a much higher standard for misappropriation than the UTSA, thereby providing more protection for trade secret holders. *See* N.C. Gen. Stat. § 66-152(1) (1997); Lao, *supra* note 23, at 1663.

[205] *See Four Reasons*, *supra* note 194, at 779-82.

[206] The court must determine what law applies to a legal dispute whenever the dispute implicates the substantive law of more than one state. *See* Hanson v. Denckla, 357 U.S. 235, 254 (1958). This is a different question than personal jurisdiction. *See id.* A court may have personal jurisdiction over a defendant yet still be obliged to apply the law of a different state. *See id.*; *see also Federal Study*, *supra* note 28, at 312.

[207] *Four Reasons*, *supra* note 194, at 776-78; Lao, *supra* note 23, at 1673. Of course, federal laws are interpreted differently in different circuits, but at least courts would be starting from the same statutory language. The Supreme Court also steps in occasionally to resolve circuit splits. U.S. Sup. Ct. Rule 10(a) (stating that the U.S. Supreme Court may review a case on a writ of certiorari where "a United States court of appeals has entered a decision in conflict with the decision of another United States court of appeals on the same important matter"); Supreme Court Procedures: Writs of Certiorari, http://www.uscourts.gov/educational-resources/get-informed/supreme-court/supreme-court-procedures.aspx (noting that the U.S. Supreme Court only accepts 100-150 of the more than 7,000 cases that it is asked to review each year).

[208] *See* JAMES POOLEY, TRADE SECRETS § 2.03[7](c) (2013) ("It is true that the similarities in substance among state enactments are far greater than the differences in language used") Even where the language of the law differs, courts' interpretations are similar. *See id.* at § 2.01[1] ("Usually what is seen as 'improper means' in Illinois will be similarly seen in California. . . .").

in cases of cyber-misappropriation are more likely to reside in a different state or even a different country than traditional defendants.[209] Further, determining where the wrong occurred may be quite difficult in the digital context when the defendant committed the wrong while located in one state, yet the actual cyber-intrusion took place on computer servers in another state. [210] As a result, choice-of-law issues become quite complicated in cyber-misappropriation cases, thereby significantly increasing the cost of litigation.[211] A civil federal law would obviate the choice-of-law problem.

In addition, suing out-of-state and out-of-country defendants is easier in federal court because of liberal discovery rules and broader jurisdictional reach. Unlike in federal courts, trial counsel do not have access to nationwide subpoenas in most state courts.[212] To give an example of the discovery challenges, a plaintiff in an Illinois court cannot depose a witness in California without petitioning both the Illinois and California courts.[213] Therefore, for jurisdictional and procedural reasons, direct access to federal courts through subject-matter jurisdiction under a federal civil trade secret law might facilitate suits against cyber-misappropriators.[214]

This would only be true, however, in a very limited number of cases because parties in cyber-misappropriation cases would generally have access to federal courts anyway. Because cyber-misappropriators are likely to be out-of-state defendants, plaintiffs can assert these claims in federal courts under their diversity jurisdiction.[215] The parties would also have access to federal courts through supplemental subject-matter jurisdiction due to the fact that cyber-misappropriation cases often involve federal claims under the Computer Fraud and Abuse Act as well other federal laws.[216]

---

[209] *See* ERIC M. DOBRUSIN & RONALD A. KRASNOW, INTELLECTUAL PROPERTY CULTURE: STRATEGIES TO FOSTER SUCCESSFUL PATENT AND TRADE SECRET PRACTICES IN EVERYDAY BUSINESS 234 (2008) ("With [new ideas and the Internet] also grew the opportunity for misappropriation of the ideas and the technological means for achieving such misappropriations.").
[210] *See* Lao, *supra* note 23, at 1668-74.
[211] *See supra* note 206.
[212] R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656, 667-68 (2008).
[213] *Id.* at 668.
[214] 28 U.S.C. § 1331.
[215] 28 U.S.C. § 1332(a). This is true as long as the amount in controversy exceeds $75,000. *Id.* If the losses through cyber-espionage are as great as advocates of strengthening trade secret law claim, then plaintiffs should not have difficulty alleging damages in this amount.
[216] 28 U.S.C. § 1367 (2006) (defining the civil procedure mechanism of supplemental jurisdiction).

In addition, a civil federal trade secret law would pose new hurdles to trade secret owners. Due to the fact that such a law would be enacted under Congress's Commerce Clause power, trade secret holders would have to show use of the trade secret in interstate commerce as a threshold matter.[217] Being forced to prove use in interstate commerce early in the litigation would increase the risk that the trade secret would be disclosed to the public.[218] To lessen this risk, trade secret owners might prefer to pursue their trade secret claims under state law.

To summarize, it is possible that in some cases, a federal law might overcome inefficiencies in the state law system. But that does not mean that a federal law must grant broader rights to trade secret holders. Given the desire among political leaders to take action on cyber-misappropriation, this may be a dangerous time for Congress to enact a federal civil trade secret law. As shown in the preceding subsection, political leaders appear to be deeply concerned about cyber-misappropriation of trade secrets – or, at least, they find it politically advantageous to appear tough on cyber trade secret theft. Consequently, countervailing concerns may get short shrift in the deliberations.

Indeed, the most likely version of a federal civil trade secret law illustrates precisely this danger. The easiest route to federalizing trade secret law would be to add a private right of action to the Economic Espionage Act (EEA). The EEA is a federal criminal statute with two main provisions.[219] The foreign espionage provision prohibits the misappropriation of trade secrets to benefit foreign governments.[220] The more general trade secret provision codified in Section 1832 of Title 18 prohibits trade secrets misappropriation generally, in terms roughly similar to the UTSA.[221] Amending the EEA to allow private parties to sue for violations of Section 1832 would effectively create a federal civil trade secret law.

---

[217] *See supra* note 206; U.S. CONST. art. I, § 8, cl. 3; 15 U.S.C. § 1127 ("'commerce' means all commerce which may lawfully be regulated by Congress");18 U.S.C. § 1832 (limiting protection to trade secrets "used in or intended for use in interstate or foreign commerce"); Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 93-102 (1998) (rejecting doctrine of "hypothetical jurisdiction" that would allow a court to rule on issues of law before adjudicating jurisdiction).

[218] SHARON SANDEEN & ELIZABETH ROWE, TRADE SECRET LAW IN A NUTSHELL § 4.10 (West 2013).

[219] The EEA does provide for civil claims by the Attorney General, but not by private parties. *See* 18 U.S.C. § 1836.

[220] 18 U.S.C. § 1831.

[221] *See* 18 U.S.C. §§ 1831, 1832, 1839; UNIF. TRADE SECRETS ACT § 1.

The additional language necessary to add a private right of action to the EEA would raise few drafting disputes because it would require no more than a sentence.[222] Tacking onto the EEA rather than creating a new statute would have the advantage of using language from a statute that has existed without major controversy for almost two decades.[223] The idea also has considerable support.

Advocates have called for a private right of action under the EEA since the act was enacted in 1996.[224] Like calls for a federal civil trade secret law generally, calls for adding a private claim to the EEA have multiplied in response to rising concern about cyber-threats. Practicing attorneys, the bipartisan commission on intellectual property law, and numerous other organizations have all recommended giving private parties the right to sue for violations of the EEA.[225] Two years ago, Senators Kohl, Coons, and Whitehouse sponsored the Protecting American Trade Secrets and Innovation Act of 2012 (PATSIA), which would have granted private parties the right to sue for violations of the existing EEA, ex parte seizure orders, and a federal version of the UTSA.[226] In June 2013, Representative

[222] For example, a bill proposed by Rep. Zoe Lofgren adds a single sentence providing a private right of action to the EEA. *See* Private Right of Action Against Theft of Trade Secrets Act of 2013, H.R. 2466, 113th Cong. (2013).

[223] The EEA was enacted in 1996. Pub. L. No. 104-294, Oct. 11, 1996.

[224] As Sen. Arlen Specter stated, "We have been made aware that available civil remedies may not be adequate to the task and that a federal civil cause of action is needed. This is an issue we need to study carefully, and will do so next year." 104 Cong. Rec. S12201, S12208 (daily ed. Oct. 2, 1996). The EEA already includes a civil cause of action in that the Attorney General may obtain an injunction for violation of the EEA. 18 U.S.C. § 1836. The EEA, however, currently has no provision for suits by private parties. *See* 18 U.S.C. §§ 1831-1836.

[225] IP COMMISSION REPORT, *supra* note 118, at 5; R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656, 678 (2008); Intellectual Property Owner's Association, Request for Public Comments on "Trade Secret Theft Strategy Legislative Review" 78 Fed. Reg. 16875 (Mar. 19, 2013), at 1, Apr. 22, 2013 *available at* http://www.regulations.gov/#!documentDetail;D=OMB-2013-0002-0001; Peter Toren, *Trade Secret Theft Strategy Legislative Review*, *available at* http://www.regulations.gov/#!documentDetail;D=OMB-2013-0002-0001; Russell Beck, Response to Request for Public Comments for Trade Secret Theft Strategy Legislative Review (78 Fed. Reg. 16875, Mar. 19, 2013) Docket number IPEC-2013-0002, Apr. 22, 2013, *available at* http://www.regulations.gov/#!documentDetail;D=OMB-2013-0002-0001.

[226] Protecting American Trade Secrets and Innovation Act of 2012, S. 3389, 112th Cong. (2012).

Zoe Lofgren introduced a bill that added a private right of action to the EEA.[227] Other similar bills are pending.[228]

III. THE COSTS OUTWEIGH THE BENEFITS OF STRENGTHENING TRADE SECRET LAW TO COMBAT CYBER-MISAPPROPRIATION

At first blush, the logic of enacting stronger trade secret laws to counter cyber-misappropriation makes sense. If the goal of the property theory of trade secret law is to balance incentives to develop useful information against public access, then trade secret law should strengthen trade secret protections to counter cyber-misappropriation. Otherwise, it would seem that the increased vulnerability of trade secrets to cyber-threats will result in decreased incentive to develop trade secrets. Logically, trade secret holders will invest less in developing useful information if that information can be easily cyber-misappropriated and used by competitors.[229] To protect the economy and innovation then, the law should strengthen trade secret rights.

But in fact, broadly strengthening trade secret laws will likely harm innovation and the economy with little compensating benefit.

First, trade secret holders will benefit little from increased rights to pursue cyber-misappropriation in the courts. Despite the evidence of growing misappropriation of business information through cyber-hacking, cases involving cyber-misappropriation constitute only a small percentage of overall trade secret cases in the courts. It may be that the litigation statistics do not reflect the percentage of cyber-misappropriation that actually occurs. However, trade secret holders are reluctant to pursue cyber-misappropriators in court for a number of reasons unrelated to trade secret law. As a result, greater rights and protections are unlikely to encourage trade secret holders to enforce their rights more vigorously in the courts.

Second, a law to increase rights and protections for all trade secret holders would dramatically tip the balance of trade secret law against public access. Follow-on development of the trade secret information would suffer, as well as other public interests in trade secret information.

---

[227] Private Right of Action Against Theft of Trade Secrets Act of 2013, H.R. 2466, 113th Cong. (2013). Notably, Representative Lofgren's bill excludes reverse engineering and independent derivation from misappropriation. *See id*.

[228] Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014); Future of American Innovation and Research Act of 2013, S. 1770, 113th Cong. (2013).

[229] Similarly under the tort theory, if increased vulnerability to cyber-misappropriation leads trade secret holders to wasteful expenditures on security, then the law should provide greater protection to trade secrets. *See* Part I.A, *supra*, for a discussion of the tort theory of trade secret law.

A. Strengthening Trade Secret Law Would Have Little Effect on Cyber-Misappropriation

As this section will explain, granting trade secret holders stronger legal rights will do little to help them protect their trade secrets. First, trade secret holders often refrain from suing cyber-misappropriators for reasons related to technical and strategic concerns, not to weaknesses in the law. Second, although a federal civil trade secrets law may offer trade secret holders some procedural advantages in suits against cyber-misappropriation, cyber-misappropriation does not pose unique substantive challenges. To the contrary, establishing a substantive claim of trade secret misappropriation based on cyber-hacking is relatively straightforward.

1. Trade Secret Holders Have Technological and Business Reasons for not Suing Cyber-Misappropriators

Trade secret holders are unlikely to sue cyber-misappropriators for a number of non-legal reasons: failure to detect the misappropriation, inability to identify the perpetrator, embarrassment, concern about disclosing the trade secret, business diplomacy, and convenience.

In many cases of trade secret misappropriation by cyber-hacking, the victim may not even realize it has been hacked.[230] Even where it is aware of the intrusion, the firm may not be able to identify whom to sue. The internet makes it relatively easy for cyber-hackers to hide their identities.[231] Cyber-intruders often route their operations through other computer systems to hide the origin of their activity.[232] And cyber-hackers increasingly share tools across the internet, making it hard to identify a group by its tactics.[233] Foreign entities even hire independent hackers to do their work for them, providing plausible deniability.[234] As a result, even sophisticated cyber-security companies struggle to identify the culprits behind cyber-intrusions.[235] Indeed, Mandiant made headlines when it

---

[230] ONCIX 2011, *supra* note 113, at 3; ONCIX, ANN. REP. TO CONGRESS ON FOREIGN ECON. COLLECTION & INDUS. ESPIONAGE v (2005); OFFICE OF THE NATIONAL COUNTER INTELLIGENCE EXECUTIVE, FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2003 at 2 (2003), *available at* http://www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.
[231] ONCIX 2011, *supra* note 113, at 1.
[232] *Id.*
[233] *Id.*
[234] *Id.*
[235] *See, e.g.*, MANDIANT, THE ADVANCED PERSISTENT THREAT, M-TRENDS 2 (2010), *available at* https://www.mandiant.com/resources/m-trends/ [hereinafter M-TRENDS 2010] (cyber-security firm admitting to inability to determine the identities of advanced persistent

managed to identify one advanced persistent threat as a unit of the Chinese army.[236] Although attribution techniques will likely improve, so will the evasion tactics of cyber-intruders.[237] In the meantime, many individual companies will not have the time or resources to find the perpetrator.

Determining whether an insider has misappropriated data is easier.[238] The insider typically has an assigned identifier. The company can simply check the computer system logs to determine what information he or she accessed.[239]

Even where trade secret holders know they have been compromised and can identify the culprit, they hesitate to pursue cyber-misappropriators because of unwillingness to publicly disclose that they have been compromised.[240] Companies generally have no obligation to report cyber-intrusions to law enforcement or intelligence agencies.[241] Except for the limited case of activists, the parties that misappropriated the trade secret try to keep their actions secret because of concerns about legal liability and a desire to maintain the competitive advantage of the trade secret.[242] As a result, information about the trade secret loss will generally not become

---

threats); SHADY RAT, *supra* note 123, at 4, 6 (cyber-security unable to identify cyber-intruder despites gaining access to the culprit's command and control server and identifying 71 of the compromised parties).

[236] *See* David E. Sanger, et al., *China's Army Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

[237] *See generally* MANDIANT APT 1, *supra* note 1.

[238] CERT 2013 SURVEY, *supra* note 46, at 11 (discussing the tools available to companies to detect insider attacks).

[239] For example, in *United States v. Min*, the discovery by the employer's IT department that the defendant employee had accessed an unusual number of documents within a few days triggered an investigation that led to criminal charges. Government's Response to Defendant's Motion for Downward Departure at 5, United States v. Min, No. 1:06-cr-00121-SLR (D. Del. Nov. 5, 2007).

[240] COMPUTER SECURITY INSTITUTE, 2010/2011 COMPUTER CRIME AND SECURITY SURVEY 24 (2011), *available at* http://www.ncxgroup.com/wp-content/uploads/2012/02/CSIsurvey2010.pdf (reporting that breached organizations did not report breaches to law enforcement because of concerns about negative publicity); OFFICE OF THE NATIONAL COUNTER INTELLIGENCE EXECUTIVE, FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2003 at 2 (2003), *available at* http://www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf

[241] *See generally* SAMUELSON LAW, TECH. & PUB. POLICY CLINIC, UNIV. OF CAL. AT BERKELEY SCH. OF LAW, *Security Breach Notification Laws: Views from Chief Security Officers* (2007) (discussing public notification laws and their effect on the information security industry), *available at* http://www.law.berkeley.edu/files/cso_study.pdf.

[242] In some cases, however, confidential information is misappropriated by posting it on the internet for public disclosure. Elizabeth A. Rowe, *Proposing a Mechanism for Removing Trade Secrets from the Internet*, 12 NO. 3 J. INTERNET L. *3 (2008).

public unless the trade secret holder files suit or otherwise publicizes the matter. Trade secret holders, however, face several disincentives against disclosure.

In general, firms are reluctant to disclose trade secret losses because of concerns about the effect on their stock price,[243] losing control of the investigation to the government prosecutors,[244] and further dissemination of the trade secret.[245] The loss of trade secrets through cyber-intrusion raises additional concerns about loss of public reputation and trust.[246] A trade secret theft by an insider who exploits access necessary for her job does not necessarily suggest incompetence. Organizations must give their insiders access to trade secrets in order to use them, and occasionally a firm employs a bad apple.[247] However, a cyber-intrusion by an outsider suggests that all data stored in the organizations' computer systems are vulnerable to cyber-attacks from around the world. This raises concerns among customers and the public at large that the organization cannot protect consumer privacy, credit card information, financial information, or any other data which members of the public have entrusted to the organization.[248] For example, a

---

[243] *See* Chris Carr & Larry Gorman, *The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act*, 57 BUS. LAW. 25, 52 (2001).

[244] *Corporate and Industrial Espionage and Their Effects on American Competitiveness: Hearing Before the Subcomm. on Int'l Econ. Pol'y & Trade of the H. Comm. on Int'l Relations*, 106th Cong. 180 (2000) (statement of Scott Charney, Partner, PricewaterhouseCoopers).

[245] *See Economic Espionage: Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 104th Cong. 7, 94 (1996) (statement of Thomas W. Brunner, Partner, Wiley, Rein & Fielding); *see generally* Gerald O'Hara, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS 241, 271 (2010).

[246] For example, a survey of chief information security officers conducted by the Samuelson Law, Technology & Public Policy Clinic at University of California-Berkeley School of Law found that all respondents were concerned that a public notification of a breach would damage their organizations' reputations and the trust behind their name. *See* SAMUELSON LAW, TECH. & PUB. POLICY CLINIC, *supra* note 241 at 15.

[247] *See* Wexler v. Greenberg, 160 A.2d 430, 435 (Pa. 1960) ("[I]t must be recognized that modern economic growth and development has pushed the business venture beyond the size of the one-man firm, forcing the businessman to a much greater degree to entrust confidential business information relating to technological development to appropriate employees.").

[248] *See* SAMUELSON LAW, TECH. & PUB. POLICY CLINIC, *supra* note 241 at 14-15. For example, a CSI/FBI survey found that 48 percent of respondents cited negative publicity as a reason for not reporting a computer security breach to law enforcement. *Id. See also* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 929 (2007) ("Companies sometimes invest in data security because they care about the regard in which they are held by outsiders, whether consumers, citizens, communities, or social activists. . . . Today, fear of unauthorized access to such information

survey showed that over three-quarters of marketing professionals believed that security breaches negatively impacted the reputations of companies.[249]

In addition, trade secret owners fear that their trade secrets will be disclosed during the litigation process.[250] Although courts may agree to issue protective orders during the pleading and discovery stages, trade secrets can still leak through these protections.[251] At the trial stage, courts hesitate to restrict public access to court proceedings because of the strong public interest in open access to judicial proceedings.[252]

Firms may also hesitate to pursue cyber-misappropriation for reasons of business diplomacy. Publicly accusing a foreign government or corporate rival of trade secret misappropriation could alienate potential business partners and offend potential customers.[253] Moreover, the advantages of doing business in a profitable market may outweigh the costs of some trade secret losses.[254]

Finally, the loss of trade secrets through cyber-misappropriation may often be a low priority for trade secret holders. Again, misappropriation of a trade secret usually does not deprive a firm of the information itself.[255] The loss to the firm is the loss of the competitive

---

and the possibility of identity theft would add another level of concern."); ONCIX 2011, *supra* note 113, at 3 ("[A]nnouncing a security breach of this kind could tarnish a company's reputation and endanger its relationships with investors, bankers, suppliers, customers, and other stakeholders.");
U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 112TH CONG., ANNUAL REPORT TO CONGRESS 10 (2012), available at http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress-Executive%20Summary.pdf.

[249] CMO COUNCIL, *Secure the Trust of Your Brand: How Security and IT Integrity Influence Corporate Reputation*, 7 (2006).

[250] SHARON SANDEEN & ELIZABETH ROWE, TRADE SECRET LAW IN A NUTSHELL § 4.10 (West 2013).

[251] *Id.* at § 4.10.1.

[252] *See, e.g.*, Citizens First Nat. Bank of Princeton v. Cincinnati Ins. Co., 178 F.3d 943, 945 (7th Cir. 1999) ("[T]he public at large pays for the courts and therefore has an interest in what goes on at all stages of a judicial proceeding. . . . That interest does not always trump the property and privacy interests of the litigants, but it can be overridden only if the latter interests predominate in the particular case, that is, only if there is good cause for sealing a part or the whole of the record in that case.").

[253] ONCIX 2011, *supra* note 113, at 3 ("Second, identifying IP theft almost necessarily requires identifying the source of the theft. If the origin of the theft is in a strategically important market for a company, then a certain level of theft may be written off as merely a 'cost of doing business' in an otherwise profitable market."); IP COMMISSION REPORT, *supra* note 118, at 23.

[254] IP COMMISSION REPORT, *supra* note 118, at 23.

[255] CSIS REPORT, *supra* note 156, at 8 ("[C]yber spying is not a zero-sum game. Stolen information is not really gone. Spies can take a company's product plans, its research

advantage that the trade secret provided.[256] By definition, a firm loses no competitive advantage when companies use its trade secret in a market in which it does not compete.[257] Although the media and the political establishment loudly deplore cyber-misappropriation from afar by foreign actors—especially foreign governments—this type of misappropriation may not concern companies without operations in these foreign countries.[258] In addition, developing a piece of complicated technology requires expertise and know-how that a trade secret misappropriator may lack.[259] Even if the companies that receive the trade secrets use that information to eventually compete, the initial trade secret holder may by that point rely on new innovations for a competitive advantage.[260] As a result, firms may decide that pursuing the loss of trade secrets to non-competitors or even potential competitors operating in remote markets is not worth the effort.

2. Strengthening Substantive Trade Secret Law Would Have Little Impact on Cyber-Misappropriation

From a legal perspective, however, suits against cyber-misappropriators do not pose greater substantive challenges than conventional trade secret cases. To the contrary, cases involving outside hacking may be easier to assert than cases involving insiders.

To prove trade secret misappropriation under the UTSA, a plaintiff must prove: 1) the information at issue derives independent economic value from not being generally known or readily ascertainable by competitors; 2) the information at issue was subject to reasonable efforts to keep it secret; and 3) misappropriation.[261] Of these, the latter two elements will be relatively easy to prove in cases involving outside cyber-hackers. The first element will involve the same challenges as in any other trade secret case.

Hacking into a database to obtain trade secrets easily satisfies the misappropriation element of a trade secret claim.[262] Again, state trade secret

---

results, and its customer lists today, and the company will still have them tomorrow. The company may not even know that it no longer has control over that information.").

[256] *Id.* at 9.

[257] Burstein, *supra* note 112, at 947.

[258] *Id.*

[259] CSIS REPORT, *supra* note 156, at 9 ("[Acquirers] may lack the advanced manufacturing capacity or skill needed to produce military or high tech products.").

[260] *See* CSIS REPORT, *supra* note 156, at 9 (noting that putting a competing product on the market containing misappropriated trade secrets may take years).

[261] *See* UNIF. TRADE SECRETS ACT § 1.

[262] Improper means include illegal conduct, E.I. DuPont De Nemours v. Christopher, 431 F.2d 1012, 1014 (5th Cir. 1970) and a number of independent laws, including the CFAA, prohibit hacking. *See, e.g.*, 18 U.S.C.A. § 1030(a)(2)(C) ("Whoever intentionally accesses

laws modeled on the UTSA effectively divide misappropriation into two types: improper means and breach of a confidence.[263] The UTSA explicitly states that "espionage through electronic means" is a form of improper means.[264] "[E]spionage through electronic means" rather clearly refers to hacking computer systems to obtain access to trade secrets and courts have adopted that interpretation.[265]

With regard to the second requirement, if the computer system could only be breached by some form of unauthorized and sophisticated cyber-hacking, then the computer system itself would not fail the requirement of reasonable efforts to maintain secrecy.[266] The trade secret holder might fail to satisfy the reasonable efforts requirement in other ways—for example, by failing to sign non-disclosure agreements with business partners—but these measures are not specific to cases involving misappropriation through a computer system. As a result, proving misappropriation of a trade secret in a case involving cyber-misappropriation does not involve additional legal challenges specific to cyber-misappropriation.

To the contrary, the features inherent to cyber-misappropriation make a claim of trade secret misappropriation relatively easy to prove. Because a trade secret holder can satisfy the misappropriation element by showing espionage through electronic means, the trade secret holder need not undertake the more complicated task of proving a breach of a confidence or one of the other more complex types of misappropriation.[267]

---

a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer . . . shall be punished . . . ."); CAL. PENAL CODE § 502(c). There may be gray areas at the boundaries concerning, for example, whether hacking in some instances constitutes permissible reverse engineering. *See* GABRIEL M. RAMSEY ET AL., 2 INTERNET LAW AND PRACTICE § 18:19 (2013). Most scenarios involving hacking are, however, indisputably a form of improper means.

[263] UNIF. TRADE SECRETS ACT § 1(2).

[264] UNIF. TRADE SECRETS ACT §§ 1(1), (2).

[265] *See, e.g.*, Physicians Interactive v. Lathian Systems, Inc., 2003 WL 23018270, *8 (E.D. Va. 2003) ("There can be no doubt that the use of a computer software robot to hack into a computer system and to take or copy proprietary information is an improper means to obtain a trade secret, and thus is misappropriation under the VUTSA."); *see also* Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1326 (S.D. Fla. 2003) (finding that hacking into a computer system constitutes misappropriation by espionage through electronic means).

[266] UNIF. TRADE SECRETS ACT § 1(4)(i).

[267] UNIF. TRADE SECRETS ACT § 1(2)(ii)(B)(II) ("'Misappropriation' means . . . disclosure or use of a trade secret of another without express or implied consent by a person who . . . at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was . . . acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use . . . ."); E.I. DuPont De Nemours v. Christopher, 431 F.2d 1012, 1016-17 (5th

Those advocating stronger trade secret laws might object that trade secret law should be strengthened not to combat outside cyber-misappropriators, but rather to counter insiders who take advantage of the digitization of trade secrets to easily collect and transfer massive amounts of information, sometimes across the globe. Many of the cases in which trade secrets were transferred to foreign countries involved employees using their access to the internet and the employer's digitized trade secrets to send trade secrets outside of the United States.[268] But again, these are relatively straightforward trade secret misappropriation cases under the UTSA. When an insider sends thousands of documents by using her insider access, it is relatively easy to show that she understood the value of those documents and her duty to maintain secrecy.[269]

3. Statistical Evidence that Strengthening Trade Secret Law Would Have Little Effect on Cyber-Misappropriation

Litigation and breach statistics support the conclusion that strengthening trade secret law would have little impact on cyber-misappropriation. Trade secret holders in fact seem to be reluctant to sue in cases of cyber-misappropriation. The statistics suggest that the number of cyber-misappropriation cases that plaintiffs bring to court is significantly smaller than the number of actual incidents of trade secret cyber-misappropriation.

Three studies indicate that cases of cyber-misappropriation are a small percentage of the total number of litigated trade secret cases. Attorneys at O'Melveny & Myers LLP conducted two studies: a study on state trade secret cases and one on federal trade cases.[270] In both, the attorneys examined all opinions that expressly decided a substantive trade

---

Cir. 1970) (holding that calculated efforts to overcome reasonable efforts to maintain secrecy are improper means).

[268] *See, e.g.*, ADMINISTRATION STRATEGY, *supra* note 192, at 5, 7; Federal Bureau of Investigation, Press Release, Former DuPont Chemist Sentenced to 14 Months in Prison for Stealing DuPont Trade Secrets, (Oct. 21, 2010), *available at* http://www.fbi.gov/baltimore/press-releases/2010/ba102110a.htm (defendant emailed trade secrets to his email account created for his new job at a Chinese university); United States v. Aleynikov, 737 F. Supp. 2d 173, 175 (S.D.N.Y. 2010) ("On his last day of employment at Goldman, June 5, 2009, Aleynikov copied, compressed, encrypted, and transferred to an outside server in Germany hundreds of thousands of lines of source code for the Trading System, including trading algorithms that determine the value of stock options.").

[269] UNIF. TRADE SECRETS ACT § 1.

[270] *State Study*, *supra* note 26; *Federal Study*, *supra* note 28.

secret law issue.[271] The federal study examined cases between 1950 and 2008, for a total of 394 cases.[272] The state study looked at cases between 1995 and 2009, resulting in 358 cases.[273] Of the state trade secret cases, 93 percent involved an insider, either an employee or a business partner.[274] The percentage was 85 percent in the federal cases.[275] Peter Toren's study of cases under the Economic Espionage Act echoes these numbers.[276] Toren reviewed all 124 prosecutions conducted by the government between the law's enactment in 1996 and 2012.[277] He found that in more than 90 percent of cases, the defendant was an insider, either an employee or business partner.[278] International numbers tell a similar story. For example, Germany's Federal Office for the Protection of the Constitution reported that approximately 70 percent of all German cases involved insiders.[279]

Although these studies did not track precisely how many cases involved cyber-misappropriation, the data about insiders and outsiders indicate that cyber-misappropriation is rarely litigated.[280] Much of the concern about cyber-misappropriation has centered on reports of outsiders, particularly foreigners, hacking into companies to misappropriate trade secrets.[281] At the outside, these cases can only constitute about 7-15 percent

---

[271] The federal study analyzed opinions from federal district courts. *Federal Study*, *supra* note 28, at 293. The state study focused instead on state appellate decisions because state trial court opinions are often unpublished or lacking in detail. *State Study*, *supra* note 26, at 63. While the two data sets are not perfect parallels since the federal study examines trial court opinions and the state study examines appeals opinions, there is no obvious reason to think that insider cases are appealed more often than outsider cases, or vice versa. As a result, the data from the studies seems at least roughly comparable.

[272] *Federal Study*, *supra* note 28, at 293.

[273] *State Study*, *supra* note 26, at 59.

[274] *State Study*, *supra* note 26, at 69.

[275] *Federal Study*, *supra* note 28, at 303.

[276] Peter J. Toren, *An Analysis of Economic Act Prosecutions: What Companies Can Learn From it and What the Government Should Be Doing About It!*, BLOOMBERG BNA PATENT, TRADEMARK & COPYRIGHT JOURNAL, 5 (Vol. 84, No. 2081) (Sep. 21, 2012).

[277] *Id.* at 1.

[278] *Id.* at 5. The correspondence between O'Melveny's federal study and Toren's study is not surprising considering that O'Melveny included EEA cases in its study, but it is a useful validation of each study's accuracy. *Federal Study*, *supra* note 28, at 297, 330.

[279] ONCIX 2011, *supra* note 113, at App. B.

[280] Toren, *supra* note 276, at 5; *Federal Study*, *supra* note 26, at 303-04 ("The data show that [concerns about misappropriation by foreign actors] may be overblown because unrelated third parties comprise a small percentage of alleged misappropriators.").

[281] *See, e.g.*, David E. Sanger, et al., *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 2, 2012, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

of litigated cases.[282] Indeed, the percentage is probably less because not all outsider cases may involve cyber-misappropriation.[283] Second, the insider cases—the vast majority of cases—involve little cyber-hacking. Insiders need not resort to cyber-hacking because they already have access.[284] As studies of insider misappropriation show, most cases of misappropriation by insiders simply involve employees or business partners taking advantage of the access available to them as part of their jobs.[285]

Statistics from other sources, however, suggest that cyber-hackers cause more breaches than the litigation statistics show.[286] This tends to confirm that trade secret holders refrain from suing in cases of cyber-misappropriation.

The relevant studies fall into two categories: company surveys and collected incident reports. With regard to the former, at least a third of surveyed companies consistently cite outsider attacks as the greatest source of risk to their proprietary information. In a 2009 survey by McAfee, for example, 51 percent of respondents cited cyber-vulnerabilities as the biggest threat to their vital information.[287] Similarly, a 2013 CERT report found that 31 percent of respondents identified external attacks as causing the most damage to their company.[288] Perhaps more concretely, about 30

---

[282] Toren, *supra* note 276, at 5; *State Study*, *supra* note 26, at 69; *Federal Study*, *supra* note 28, at 303.

[283] ASIS INTERNATIONAL, TRENDS IN PROPRIETARY INFORMATION LOSS 28 (June 2007), *available at* https://foundation.asisonline.org/FoundationResearch/Publications/Documents/trendsinproprietaryinformationloss.pdf [hereinafter ASIS 2007 SURVEY]. Survey respondents only reported 16 threats to proprietary information by outsiders involving either electronic interception or penetration. *Id.* at 34 (noting that only 33 percent of incidents it surveyed involved records in electronic format).

[284] Verizon reported that most cases of insider data breach involve insiders misusing their privileges. VERIZON 2013 REPORT, *supra* note 46, at 6; CERT 2013 SURVEY, *supra* note 46, at 10.

[285] VERIZON 2013 REPORT, *supra* note 46, at 6; CERT 2013 SURVEY, *supra* note 46, at 10.

[286] *See* CERT 2013 SURVEY, *supra* note 46, at 3 (survey); MCAFEE UNSECURED ECONOMIES, *supra* note 132, at 2 (survey); VERIZON 2013 REPORT, *supra* note 46, at 8-10 (collected incident report).

[287] MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 9 (Jan. 29, 2009) *available at* http://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf [hereinafter MCAFEE UNSECURED ECONOMIES].

[288] CERT 2013 SURVEY, *supra* note 46, at 10. The CERT Study surveyed over 500 US executives, security experts, and others from the public and private sectors. *Id.* at 3. The CERT survey may not be as relevant to trade secret misappropriation because it asked more generally about damage from "electronic crime," which might encompass a range of crimes other than trade secret misappropriation, such as destructive viruses, privacy breaches, and theft of financial information. *Id.* at 10.

percent of the respondents in a 2007 ASIS Foundation study stated that outsiders caused their single most significant incident of loss.[289]

The most detailed public report collecting incidents of breaches, Verizon's 2013 Data Breach Investigations Report, tells a more startling story about outsider breaches than the surveys. Based on 125 incidents of data breaches involving trade secret compromises, Verizon found that 96 percent involved external actors and only 4 percent involved insiders.[290] Methodological differences between Verizon's report and the survey reports, however, suggest that the truth is somewhere in between. Unlike the surveys, Verizon analyzed confirmed breaches.[291] Breached organizations generally supplied this information to Verizon in the course of investigations into the nature, extent, and possible remediation of the breach.[292] As a result, the information is skewed toward outsider cyber-hacking because organizations typically have less need for forensic services in cases of insider breach. In cases of insider breach, the breached organization generally already knows how the insider got access and the extent of that access because the organization itself gave the permissions.[293]

It bears noting at this point that insider misappropriation still appears to make up the lion's share of trade secret misappropriation. In the 2009 survey by McAfee and 2007 survey by the ASIS Foundation, 68 percent and 67 percent, respectively, of respondents reported that insiders constituted the greatest threat to vital information.[294] Indeed, an analyst at

---

[289] ASIS 2007 SURVEY, *supra* note 283, at 33. One hundred and forty-four companies, representing a diverse array of businesses, responded to the ASIS Survey in 2006, although less than that number responded to this specific question. *Id.* at 6, 33. This question specifically asked about the single-most-significant successful attempt to compromise or gain unauthorized access to each respondent's proprietary and trade secret information during 2005. *Id.* at 6.

[290] VERIZON 2013 REPORT, *supra* note 46, at 19, fig. 10. Additional analysis conducted on raw data supplied by Verizon is on file with the author.

[291] VERIZON 2013 REPORT, *supra* note 46, at 4.

[292] About 10 percent of the breaches were reported directly to Verizon by the organization experiencing the breach, usually in the course of receiving forensic services from Verizon's forensic consulting practice. The rest of the data came from a range of other organizations—including law enforcement agencies, incident handling entities, and other forensic service firms—most of which also obtained the information in the course of investigations. Interview with Wade Baker, Verizon, Verizon RISK Team (July 5, 2013) (Mr. Baker participated in compiling the report); VERIZON 2013 REPORT, *supra* note 46, at 4.

[293] Interview with Wade Baker, *supra* note 292; VERIZON 2013 REPORT, *supra* note 46, at 4

[294] MCAFEE UNSECURED ECONOMIES, *supra* note 287, at 9; ASIS 2007 SURVEY, *supra* note 283, at 33. In the ASIS survey, this question specifically asked about the single-most significant successful attempt to compromise or gain unauthorized access to the respondent's organization's proprietary and trade secret information during 2005. *Id.* at 6.

the technology consulting firm Gartner estimated employees accounted for about 70 percent of computer system intrusions that resulted in a loss.[295] The 2013 CERT survey found that a greater number of respondents identified insider crimes (34 percent) as causing more damage to an organization than external attacks (31 percent).[296] Insider attacks appear to be more damaging than outsider attacks because insiders know better what information is valuable and how to find it.[297] Therefore, even if trade secret holders for some reason began to pursue cyber-misappropriation more vigorously, a large number of cases would still involve insider misappropriation.

In short, bolstering trade rights would likely have little effect on cyber-misappropriation. But, as the next section discusses, it would affect other forms of trade secret misappropriation.

B. Costs of Strengthening Trade Secret Law by Adding a Private Right of Action to the EEA

Due to the fact that cyber-misappropriation poses no unique substantive legal challenges, strengthening trade secret law will not facilitate suits against cyber-misappropriation specifically. Instead, trade secret holders would simply find pursuing trade secret misappropriation easier in all cases. However, tipping the balance of trade secret law in favor of trade secret holders generally will harm other interests at stake in trade secret law without the compensating effect of targeting cyber-misappropriation.

The McAfee survey involved IT professionals from more than 1,000 organizations in U.S., U.K., Japan, China, India, Brazil and the Middle East. MCAFEE UNSECURED ECONOMIES, *supra* note 287, at 2, 5. 68 percent of the respondents cited "insider threat" as the top threat to vital information. *Id.* at 9.

[295] Bob Tedeschi, *Crime is Soaring in Cyberspace, But Many Companies Keep it Quiet*, N.Y. TIMES, Jan. 27, 2003, http://www.nytimes.com/2003/01/27/business/e-commerce-report-crime-soaring-cyberspace-but-many-companies-keep-it-quiet.html.

[296] CERT 2013 SURVEY, *supra* note 46, at 9-10 ("While most of the media cybercrime reporting has been on remote network attacks over the Internet, survey results show that among respondents answering insider-related questions, insiders were deemed more likely to be the sources of cyberattacks."). The CERT Study surveyed over 500 U.S. executives, security experts, and others from the public and private sectors. *Id.* at 3.

[297] As the CERT Study observed: "These insiders are likely to be one step ahead of external threat actors because they tend to already know what the company's crown jewels are: those assets that drive cash flows, competitive advantage, and shareholder value. They also know where they reside on the networks and how to gain access to them for the purposes of theft, disclosure, or destruction." *Id.* at 10; *see also* MCAFEE UNSECURED ECONOMIES, *supra* note 287, at 9 ("Data thefts by insiders tend to have greater financial impact given the higher level of data access.").

The addition of a private right of action to the EEA illustrates the harmful effects of strengthening trade secret law. The EEA bolsters trade secret protection in five major ways: it broadens the scope of misappropriation by 1) prohibiting reverse engineering and 2) defining misappropriation as unauthorized taking, 3) expands what constitutes trade secret information, 4) creates causes of action for attempts and conspiracy, and 5) bases trade secret rights on a property theory.[298]

Most perniciously, the EEA broadens what constitutes misappropriation. Due to the fact that cyber-misappropriation is clearly a form of improper means under current law, a broader definition of misappropriation only facilitates trade secret suits against other sorts of trade secrets misappropriation. And, by creating liability for new forms of conduct, the EEA causes collateral damage to other interests.

The EEA version of misappropriation is broader than that of the UTSA in two ways. First, the EEA appears to prohibit many forms of reverse engineering.[299] Under the UTSA and the common law, divining a trade secret by reverse engineering is a proper means for acquiring a trade secret and therefore does not trigger liability.[300] The EEA does not

---

[298] These points are discussed in more detail below. The statute also strengthens trade secret law in several more minor ways. It includes more types of information in its enumeration of information that qualifies for trade secret protection than the UTSA. *See* 18 U.S.C. § 1839(3); UNIF. TRADE SECRETS ACT § 1(4). In practice, however, this may not make a difference because the UTSA categories are so broad that a court might interpret them to cover the same types of information enumerated by the EEA. *See* 18 U.S.C. § 1839(3); UNIF. TRADE SECRETS ACT §1(4). The EEA may also protect general skills and knowledge in an employee's head as a trade secret. *See* Moohr, *supra* note 53, at 878 ("[T]he EEA may be read to protect trade secrets that exist only in the mind of the holder against misappropriation through memorization by another."); *see also* James H.A. Pooley et al., Understanding the Economic Espionage Act of 1996, 5 TEX. INTELL. PROP. L.J. 177, 190-91 (1997). For general discussions of how the EEA differs from the UTSA and state trade secret law generally, *see* Moohr, *supra* note 53 ("[A]n analysis of specific provisions of the EEA shows that—in contrast to common law—the new federal law of trade secrets offers broad protection to holders of such information. . . ."); 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, 204-206 (2013) ("Criminal laws are often narrower than their civil analogues, but in a wide range of areas the EEA pushed theft of trade secrets further than the civil—and even state criminal—laws had."); James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177 (1997).

[299] *See supra* note 80 and accompanying text for a description of reverse engineering. *See also* Pooley, *supra* note 298, at 195-96.

[300] *See* UNIF. TRADE SECRETS ACT, Comment to § 1 ("Proper means include: . . . Discovery by "reverse engineering", that is, by starting with the known product and working backward to find the method by which it was developed.") Courts have accepted the principle of reverse engineering as a form of proper means to acquire a trade secret for

expressly prohibit reverse engineering; it prohibits copying, duplicating, sketching, drawing, and altering a trade secret without authorization—actions necessary for many forms of reverse engineering.[301] For example, reverse engineering a computer program almost always involves making an unauthorized copy of the program.[302] Likewise, figuring out how a mechanical device works may require sketching, drawing, duplication, or alteration.[303] The EEA thus effectively prohibits one of the most important ways in which trade secrets legally enter the public domain.[304] By prohibiting many forms of reverse engineering, the EEA restricts follow-on innovation. Specialists cannot legally access useful information embedded in a trade secret holder's products to build on and improve them. The public interests suffers due to the slowing of innovative progress and reduced competition among players in the same industry to produce better products and services based on the useful information in the trade secret.

Second, the EEA collapses the improper means and breach of confidence categories of misappropriation in the UTSA into one broader form of misappropriation, the unauthorized taking of a trade secret.[305] Under the UTSA, misappropriation by improper means creates liability against the world for any wrongful action.[306] Misappropriation by breach of confidence creates a right only against parties to an agreement of confidentiality. Replacing these two forms of misappropriation with liability for any unauthorized taking essentially combines the broader features of each: the right against the world with liability for acting without permission. In sum, the EEA creates a right against the world for any unauthorized use of a trade secret, with the caveat that the defendant must know that her actions will injure the trade secret holder.[307]

---

more than a century; *See, e.g.*, Tabor v. Hoffman, 23 N.E. 12, 13 (1889); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974); Craig L. Uhrich, *The Economic Espionage Act—Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. & TECH. L. REV. 147, 167 n.160 (2001).

[301] *See* 18 U.S.C. §§ 1831(a)(2), 1832(a)(2).

[302] *See, e.g.*, Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1525-26 (9th Cir. 1992); *see generally* Andrew Johnson-Laird, *Reverse Engineering of Software: Separating Legal Mythology From Actual Technology*, 5 SOFTWARE L.J. 331 (1992) (describing software reverse engineering).

[303] *See* Pooley, *supra* note 298, at 195.

[304] *Cf.* Moohr, *supra* note 53, at 911-12 ("Reverse engineering . . . is generally viewed as crucial to maintaining access to information . . . .").

[305] *See* 18 U.S.C. § 1832(a); UNIF. TRADE SECRETS ACT § 1(2).

[306] *See* UNIF. TRADE SECRETS ACT § 1(1). Liability for misappropriation by improper means does not require a relationship between the trade secret holder and the misappropriator. *See id.*

[307] *See* 18 U.S.C. § 1832(a).

As a result, the EEA's version of misappropriation criminalizes many forms of conduct that would be deemed fair competition and therefore lawful under the UTSA.[308] For example, observing a competitor's operations from across the street, entering a competitor's store to record the prices on its products, and studying a competitor's behavior to learn its strategies would all qualify as misappropriation under the EEA.[309] Such activities are now considered ordinary business intelligence and necessary for vigorous competition. Like the prohibition on reverse engineering, therefore, the EEA's broader definition of misappropriation restricts competition, to the detriment of the public.

The third way in which the EEA bolsters trade secret rights is by employing a broader definition of what constitutes a trade secret. Broadening the definition of a trade secret, unlike broadening the definition of misappropriation, facilitates claims of cyber-misappropriation by making it easier to prove that the information taken by a cyber-hacker was a trade secret. Again, to establish a trade secret claim, the plaintiff must prove two elements: that she possessed a trade secret and that the trade secret was misappropriated.[310] In a case of cyber-misappropriation, the misappropriation element is generally straightforward, but the trade secret element raises the same challenges as in other trade secret claims.

The EEA broadens the definition of a trade secret by using the public as the measure of secrecy.[311] Under the UTSA, to qualify as a trade secret, information must "derive independent economic value" from "not being generally known to and not being readily ascertainable" by competitors.[312] The EEA uses the same language but replaces competitors with "the public."[313] Interpreted broadly to mean "the public at large," as

---

[308] Pooley, *supra* note 298, at 193.

[309] *See id.* at 192-93 (noting that the language of the EEA "might encompass the sort of lawful business espionage that has long been permitted by civil trade secrets law—conduct such as observing a competitor's property from across the street."). The information gathered through such efforts, however, might not qualify as a trade secret because it might not be deemed subject to reasonable efforts at secrecy. *Cf.* 18 U.S.C. § 1839(3)(A).

[310] 18 U.S.C. § 1832(a), UNIF. TRADE SECRETS ACT § 1; 1 MELVIN JAGER, TRADE SECRETS LAW § 5:5 (2013) (Jager further divides the misappropriation inquiry into two separate elements).

[311] *See* 18 U.S.C. § 1839(3)(B).

[312] The language used is: "other persons who can obtain economic value from [the trade secret's] disclosure or use." UNIF. TRADE SECRETS LAW § 1(4)(i). Logically, however, these persons will be competitors because they economically benefit by using the trade secret to better compete with the original trade secret holder. *See* United States v. Hsu, 155 F.3d 189, 196 (3rd Cir. 1998).

[313] *See* 18 U.S.C. § 1839(3)(B).

some courts have done,[314] this change expands what information qualifies as a trade secret. The information known to competitors about a particular industry will naturally be greater than the information known to the public at large about that industry.[315] In most industries, engineers, scientists, and other specialists share a body of knowledge of which the public is ignorant.[316] As a result, the EEA protects more information as a trade secret.

Again, this harms competition, particularly employee mobility. The EEA's broader delineation raises the specter that employees could be liable for taking any industry-specific information with them to a competitor, even if all the competitors already had that information.[317] In short, an employer could use the EEA simply to prevent employees from leaving.[318] This would have a devastating impact on employee mobility and the cross-pollination effect so important to a culture of innovation.[319]

Moreover, the cost to competition of the EEA's expansion of the trade secret definition likely outweighs any benefit to victims of cyber-misappropriation. In a civil claim under the EEA, a plaintiff could establish a claim for the taking of a broader range of information than under the

---

[314] United States v. Hsu, 155 F.3d 189, 196 (3rd Cir. 1998) (interpreting "the public" to refer to "the general public").

[315] *See* Julie Piper, *I Have a Secret?: Applying the Uniform Trade Secrets Act to Confidential Information that Does Not Rise to the Level of Trade Secret Status*, 12 MARQ. INTELL. PROP. L. REV. 359, 365-66 (2008) (describing information in terms of concentric circles of availability to competitors in an industry). Courts are unclear as to whether "the public" in the EEA refers to the general public or to the specialized, well-informed public in a particular industry. *Compare* United States v. Lange, 312 F.3d 263, 266-68 (7th Cir. 2002) ("[O]ne could say instead that 'the public' is shorthand for the longer phrase, which then would be read as 'the economically relevant public'—that is, the persons whose ignorance of the information is the source of its economic value."), *with* United States v. Hsu, 155 F.3d 189, 196 (3d Cir. 1998) ("The EEA, however, indicates that a trade secret must not be generally known to, or readily ascertainable by, the general public. . . .") However, the language at least gives rise to the possibility that courts will interpret "the public" as "the general public." *See* Hsu, 155 F.3d at 196.

[316] *See* United States v. Lange, 312 F.3d 263, 267 (7th Cir. 2002) ("A problem with using the general public as the reference group for identifying a trade secret is that many things unknown to the public at large are well known to engineers, scientists, and others. . . .").

[317] *See* 18 U.S.C. § 1839(3)(B).

[318] The EEA's legislative history indicates that it was not intended to prevent a person from using general business knowledge to compete with a former employer. For example, it provides that employees "who change employers or start their own [company] should be able to apply their talents without fear of prosecution." 142 CONG. REC. S12213 (daily ed. Oct. 2, 1996) (Managers' Statement for H.R. 3723, The Economic Espionage Bill). Nevertheless, the plain language of the statute belies the legislative history. *See* 18 U.S.C. § 1839(3)(B).

[319] *See* Gilson, *supra* note 74, at 620-29 (cautioning against restricting employee mobility because the dampening of knowledge spillovers may hamper innovation and growth).

UTSA.[320] She could prove trade secret misappropriation not only in cases involving information not known to the industry, but also in cases involving the broader category of information not known to the public. For example, Avogadro's number—the number of molecules per mole of gas—is not known to the general public, but would certainly be known to chemists.[321] As the Seventh Circuit observed in *United States v. Lange*, taking Avogadro's number from a chemical company without authorization could constitute misappropriation under the plain language of the EEA.[322] But what does it benefit the plaintiff to win such a claim? If she is in the chemical industry, her competitors already have the information.[323] If she is not in the chemical industry, the information is of no use to her. In short, the EEA's broad definition of trade secrets would offer little help with protecting information that actually provides a competitive advantage. It would, however, help companies stifle competition by preventing employees from working for competitors or starting a competing business.

Fourth, the EEA strengthens trade secret law by prohibiting both attempts and conspiracies to misappropriate trade secrets, neither of which gives rise to liability under the UTSA.[324] As a result, defendants would face liability for a much broader range of conduct under the EEA than under the UTSA.[325] For example, in *United States v. Hsu*, the Third Circuit held that there is no need to prove the existence of a trade secret in an attempt or conspiracy charge under the EEA.[326] The court reasoned that the attempt and conspiracy charges only require proof that the defendant believed the information to be a trade secret, "regardless of whether the information actually qualified as such."[327]

The attempt and conspiracy provisions in the EEA raise the disturbing possibility that a plaintiff could use the EEA to protect information that lacked trade secret status. As long as the defendant believed the information was a trade secret, for example, she could be liable

---

[320] *See* 18 U.S.C. § 1839(3)(B); UNIF. TRADE SECRETS LAW § 1(4)(i).
[321] 312 F.3d 263, 267 (7th Cir. 2002).
[322] *See id.*
[323] As a practical matter, she could not prove any actual damages since the information would not give her competitors any additional advantage.
[324] 18 U.S.C. §§ 1832(a)(4)-(5); *see* UNIF. TRADE SECRETS ACT (no provisions creating liability for attempts or conspiracy).
[325] *See* 18 U.S.C. §§ 1832(a)(4)-(5); UNIF. TRADE SECRETS ACT.
[326] United States v. Hsu, 155 F.3d 189, 203 (3rd Cir. 1998); *see also* United States v. Roberts, 3:08-CR-175, 2009 WL 5449224 (E.D. Tenn. Nov. 17, 2009), *report and recommendation adopted*, 3:08-CR-175, 2010 WL 56085 (E.D. Tenn. Jan. 5, 2010), *aff'd sub nom.* United States v. Howley, 707 F.3d 575 (6th Cir. 2013).
[327] United States v. Hsu, 155 F.3d 189, 203 (3rd Cir. 1998). The court concluded that the defense of legal impossibility did not apply. *Id.*

for taking information in the public domain. Again, it is hard to see how this feature of the EEA addresses the problem of cyber-misappropriation. The public concern in cyber-misappropriation is the taking of real secrets—such as when the Chinese army hacked into American computer systems and steals secret technology blueprints—not the taking of information in the public domain.[328]

In civil law, attempt and conspiracy claims lose much of their force because the plaintiff can usually only recover the damage actually caused by the defendant's actions.[329] Where the defendant does not actually succeed in misappropriating a trade secret, the plaintiff will struggle to prove actual damages. Nevertheless, in an attempt or conspiracy claim, the plaintiff might still be damaged if the information is valuable but did not quite qualify for trade secret protection.[330] The attempt and conspiracy provisions, therefore, raise the possibility that the EEA would extend trade secret protection to information now in the public domain. This could harm competition, innovation, and free speech.

Fifth and finally, the EEA bolsters trade secret holder's rights by basing trade secret rights firmly on a property theory, rather than the more traditional tort theory.[331] First, the language of the EEA clearly indicates that trade secret rights under the statute are based on a property interest. Instead of referring to the trade secret holder as the "rights holder," the

---

[328] MANDIANT APT 1, *supra* note 1 at 3.

[329] *See, e.g.*, Matthies v. Positive Safety Mfg. Co., 628 N.W.2d 842, 852 (Wis. 2001) ("It is the fact and date of injury that sets in force and operation the factors that create and establish the basis for a claim of damages."); Cockings v. Austin, 898 P.2d 136 (Okla. 1995) ("A negligent act that does not cause damage will not support the imposition of liability.").

[330] *See* Julie Piper, *I Have a Secret?: Applying the Uniform Trade Secrets Act to Confidential Information that Does Not Rise to the Level of Trade Secret Status*, 12 MARQ. INTELL. PROP. L. REV. 359, 366 (2008) (classifying valuable information in tiers, not all of which would qualify as trade secrets); Robert Unikel, *Bridging the "Trade Secret" Gap: Protecting "Confidential Information" Not Rising to the Level of Trade Secrets*, 29 LOY. U. CHI. L.J. 841, 844 (1998) (explaining that there is confidential information that does not technically rise to the level of a trade secret yet continues to be valuable within an industry).

[331] The First Restatement of Torts, the Third Restatement of Torts, the UTSA, and most state law accepts the tort theory of trade secret rights. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939) (rejecting the property theory in favor of a general duty of good faith); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 reporters' note, cmt. b, 440 (1995) (listing cases); UNIF. TRADE SECRETS ACT § 1 commissioners' cmt. (amended 1985), 14 U.L.A. 438 (1990) ("One of the broadly stated policies behind trade secret law is 'the maintenance of standards of commercial ethics.'"); 1 MELVIN F. JAGER, TRADE SECRETS LAW § 1:3, n.16 (noting that standards of fairness and commercial morality continue to be the touchstone of trade secret law in the courts and listing cases).

more common formulation under state law, it refers to the trade secret "owner."[332] It uses the terms "theft" and "steal," implying that what is taken is property.[333] It even employs the word "convert" although the tort of conversion has historically been limited to the taking of tangible property.[334] These terms do not appear in the UTSA or the Restatements.[335] Second, the legislative history bears out this interpretation. The House Report explicitly categorizes trade secrets as a type of "property" similar to patents and copyrights.[336] Third, the EEA treats trade secret rights like property. The prohibitions against unauthorized takings and many forms of reverse engineering effectively create a trade secret right against the world more akin to a property right than a duty-based right of confidence.[337] If the EEA became the basis for civil trade secret law, the courts would follow Congress's clear intent by interpreting the statute to grant trade secret holders property rights across the country.[338]

Although the two theories are largely complementary,[339] a purely property-based approach confers stronger rights on trade secret holders. As Pamela Samuelson observed in her study on propertizing information, "the word property is a very powerful metaphor that radically changes the stakes in legal disputes."[340]

---

[332] 18 U.S.C. §§ 1832(a), 1839(3)(A), 1839(4); *see* Rochelle Cooper Dreyfuss, *Trade Secrets: How Well Should We Be Allowed to Hide Them? The Economic Espionage Act of 1996*, 9 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 8 (1998) (observing that the concept of owner, as opposed to rights holder, is unknown in state trade secret law).

[333] 18 U.S.C. §§ 1832 ("theft"); 1831(a)(1) ("steals"); 1832(a)(1) ("steals"); 1831(a)(3) ("stolen"); 1831(b) ("stolen"); 1832(a)(3) ("stolen").

[334] Val D. Ricks, Comment, *The Conversion of Intangible Property: Bursting the Ancient Trover Bottle with New Wine*, 1991 B.Y.U. L. REV. 1681, 1682 (1991).

[335] Note the exception of the Third Restatement of Unfair Competition, which uses the term "owner" and "own." The Third Restatement, however, does not yet appear to be adopted by the courts. Lao, *supra* note 23 at 1650.

[336] H.R. REP. NO. 104-788, at 4 (1996) ("This category of property includes patented inventions, copyrighted material, and proprietary economic information.").

[337] Pooley, *supra* note 298, at 193.

[338] Due to the fact that the majority of states now take a tort theory approach to trade secrets law, the EEA would effectively change the law in most states. 1 MELVIN F. JAGER, TRADE SECRETS LAW § 1:3 n.16 (listing cases by states in which the tort theory predominates).

[339] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178-79 (7th Cir. 1991).

[340] Pamela Samuelson, *Information as Property: Do Ruckelshaus and Carpenter Signal a Changing Direction in Intellectual Property Law?*, 38 CATH. U. L. REV. 365, 398 (1988–1989).

Property rights tend to carry more weight against free speech rights than tort concerns.[341] Indeed, some have argued that property rights in trade secrets trump free speech rights altogether, an argument not advanced with regard to unfair competition.[342] By basing trade secret rights on a property interest, for example, the Supreme Court of California determined that free speech concerns had no place in the trade secret injunction analysis.[343] In contrast, numerous courts, including the U.S. Supreme Court, have concluded that free speech interests must be weighed against trade secret rights on the grounds that the trade secret right is based merely on an economic interest.[344]

Property also confers important rights under the Constitution. In *Ruckelshaus v. Monsanto*, for example, the Supreme Court concluded that because Monsanto held a trade secret right in its pesticide data, regulators' requests for the data were an unconstitutional taking of Monsanto's property under the Takings Clause of the Fifth Amendment.[345] Natural gas companies have since relied on this holding to deflect requests from environmentalists for information about their hydraulic fracturing practices.[346] In short, the trade-secrets-as-property approach results in a strong version of trade secret law, with significant implications for free speech, the public domain, and other concerns like the environment.

As in the other areas in which the EEA expands trade secret rights, the reframing of a trade secret right as a property interest would have little effect on cyber-misappropriation claims. The core concern in cyber-misappropriation is the taking of trade secrets by hackers who sell them to

---

[341] Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 789 (2007).
[342] *See id.* at 811.
[343] *Id.* at 803-04 ("The importance of the trade-secrets-as-property-rights argument as a justification for lowering the level of scrutiny in trade secret/First Amendment cases is evident from the more than twenty references to property rights in core parts of Justice Brown's First Amendment analysis.").
[344] *See* CBS, Inc. v. Davis 510 U.S. 1315, 1318 (1994) (referring to disclosure of a trade secret as an "economic harm" without reference to property rights); *see also* Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219, 225 (6th Cir. 1996) (referring to the desire to avoid disclosure of a trade secret as mere "commercial self-interest"); Bridge C.A.T. Scan Assocs. v. Technicare Corp., 710 F.2d 940, 945-46 (2d Cir. 1983) (holding no exception from prior restraint doctrine for trade secrets).
[345] Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1003-04 (1984). The Court found that trade secrets were "property," explaining that "[t]rade secrets have many of the characteristics of more tangible forms of property. A trade secret is assignable. A trade secret can from the res of a trust, and it passes to a trustee in bankruptcy." *Id.* at 1002-04.
[346] *See* Michael A. Greene, *Spilling Secrets: Trade Secret Disclosure and Takings in Offshore Drilling Regulation*, 17 RICH. J.L. & TECH. 15, *4-6 (2011).

competitors, especially foreign competitors.[347] These parties have no free speech defense and serve no compelling public interest. Therefore, a property right in trade secrets fails to facilitate claims against such defendants.

As a criminal law, the EEA may not offer more protection to trade secrets than current state civil law. This is because the standard of proof under a criminal statute—guilt beyond a reasonable doubt—is much higher than the preponderance of the evidence standard in the UTSA and other civil trade secret claims.[348] Creating a private right of action for violations of the EEA would change that. Defendants would face liability for violating the EEA under only the preponderance of evidence standard. The stronger rights and protections provided by the EEA would result in a much stronger form of civil trade secret law than the existing civil law.

In short, if the purpose of adding a private right of action to the EEA is to decrease cyber-misappropriation, it fails miserably. At the same time, it imposes significant costs on other interests. Of course, by strengthening trade secret law generally, a civil version of the EEA might help trade secret holders protect their information against other types of misappropriation. The current outcry over trade secret misappropriation, however, focuses on the cyber-hacking of trade secrets. By that measure, the costs outweigh the benefits of adding a private right of action to the EEA or otherwise bolstering trade secret holder's rights.

The dangers are not limited to laws that call themselves trade secret laws. In some jurisdictions, for example, the Computer Fraud and Abuse Act (CFAA) is effectively a civil federal trade secrets law. The CFAA's broadest provision prohibits "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss."[349] On its face, the CFAA might appear to be simply an anti-hacking statute. Some courts, however, have interpreted the CFAA to create liability for employees who access data in violation of a duty of loyalty or confidentiality to their employers.[350] In such cases, the employees do not

---

[347] *See supra* Part II.

[348] *In re* Winship, 397 U.S. 358, 361-62 (1970) (establishing the proof beyond a reasonable doubt standard in criminal cases); Apprendi v. New Jersey, 530 U.S. 466, 466 (2000) (reaffirming the same standard); MCCORMICK ON EVIDENCE 957 (Edward William Cleary ed., 3d ed. 1984) (noting that civil cases apply the preponderance of evidence standard); *see also* FLEMING JAMES, JR. & GEOFFREY C. HAZARD, JR., CIVIL PROCEDURE 316-17 (3d ed. 1985).

[349] 18 U.S.C. § 1030(a)(5)(C).

[350] *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that an employee exceeds authorized access under the CFAA if he accesses information for a nonbusiness reason in violation of the employer's computer use policy); Int'l Airport

hack their employers' computers in the sense of circumventing technological protections. Rather, they take advantage of access privileges granted in the course of their employment.[351] Not all courts have adopted this approach. Some courts have construed the CFAA more narrowly, finding that the CFAA was intended to cover only unauthorized access to computers and not unauthorized use of information.[352]

The broad theory effectively creates a parallel cause of action to trade secret misappropriation. This interpretation of the CFAA, however, is even broader than trade secret law because it is not limited to protecting information that would qualify for trade secret information.[353] The misuse of any information in breach of a duty of loyalty to the employer might qualify.[354]

Leaving aside the controversy as to how the CFAA should be interpreted, one implication of this paper is that the CFAA should not be construed broadly merely to counter cyber-misappropriation of trade secrets. By creating liability for unauthorized access to a computer, the narrow interpretation of the CFAA already targets hacking. The broad

---

Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (holding that Section 1030(a)(5)(A) of the CFAA was violated through unlawful access when the agency relationship terminated because the employee breached his duty of loyalty by destroying files that were employer property); Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 45-46 (D. Mass. 2009) (holding that employee violated CFAA by using and abusing information in breach of his duty of loyalty to his employer).

[351] *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006) (employee had access to data at issue through employer-granted laptop); Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 45-46 (D. Mass. 2009) (employee had unrestricted access to the information at issue due to his position as Vice President of North American Sales).

[352] *See* United States v. Nosal, 676 F.3d 854, 859, 863 (9th Cir. 2012).

[353] *See* Stephanie Greene & Christine Neylon O'Brien, *Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct under the Computer Fraud and Abuse Act*, 50 AM. BUS. L.J. 281, 329 (2013) (noting that the evidentiary requirements and elements of proof of a CFAA claim are far lower than in a traditional trade secret misappropriation claim).

[354] *See* Rodriguez, 628 F.3d at 1263; *see* UTSA § 1(4). Another controversial issue is whether misusing data meets the "damage or loss" requirement for a CFAA claim. *See* Consulting Prof'l Res., Inc. v. Concise Techs., LLC, No. 09-1201, 2010 U.S. Dist. LEXIS 32573, at *20 (W.D. Pa. Mar. 9, 2010) (noting that the debate over "what constitutes 'damage' under the CFAA falls victim to similar debate" as the conflict over interpreting authorization terms). Some courts have held that misappropriation of data does not satisfy the "loss" requirement of the CFAA and that the CFAA should be limited to hacking that causes some physical loss or disruption in service. *See, e.g.*, Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *26 (M.D. Fla. Aug. 1, 2006) (holding that copying confidential information is not damage under the CFAA).

interpretation not only creates liability for hacking, but also potentially creates liability for any unauthorized taking of data. This is unnecessary to discourage outsider cyber-hacking. At the same time, it may cause collateral damage by discouraging legitimate competition. For example, in a worst case scenario, even copying information from a public website in violation of a cease and desist letter could be considered a violation of the CFAA.[355]

As the CFAA shows, laws need not be named trade secret laws to upset the balance of policies at stake in trade secret law. The courts and legislature must be careful not to expand laws against hacking to create laws that unnecessarily prevent the free flow of information.

CONCLUSION

Despite the alarmist rhetoric, the threat of cyber-misappropriation does not merit the bolstering of trade secret rights. Instead, trade secret holders would likely take advantage of increased rights to pursue other forms of misappropriation. As the example of adding a private right of action to the EEA illustrates, strengthening trade secret rights would have significant costs. The vitality of our economy depends heavily on vigorous competition between private companies, worker mobility, and follow-on innovation. Meanwhile, the vitality of our society requires free speech and the availability of information important to public concerns. We should not risk killing the golden goose for a non-existent egg.

[355] Craigslist Inc. v. 3Taps Inc., 2013 WL 1819999, at *4 (N.D. Cal. 2013) (denying a motion to dismiss a CFAA claim where defendants scraped information from plaintiff's website despite a cease and desist letter and various efforts to block access).