Washington and Lee Law Review Online

Volume 72 | Issue 2 Article 6

12-1-2015

School Boy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation

David S. Levine
Elon University School of Law

School Boy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation

David S. Levine*

Information technology has revolutionized information storage and retrieval. The Internet and its connected devices have revolutionized how people and entities create, consume, and share information. Naturally, this same technology has also created an arms race between entities that want to keep secrets and those who want unauthorized access to them.[1] U.S. industry, and anyone whose secrets (or private information) are outside a human brain, are fixed in the middle of this conflict.[2] At the center of the problem, and the solution, is the vexing question of how to improve U.S. corporations' cybersecurity.

As a result, there is a fairly recent panic around how the government should address the "cybersecurity" problem.[3] Within

* David S. Levine is an Associate Professor at Elon University School of Law, a Visiting Research Collaborator at Princeton's Center for Information Technology Policy, and an Affiliate Scholar at Stanford Law School's Center for Internet and Society. David also hosts Hearsay Culture on KZSU-FM Stanford (hearsayculture.com). Thanks to Merima Mustafic for her research assistance, Sharon Sandeen for her comments, and Emily Tichenor and the editors and staff of the *Washington and Lee Law Review* for hosting this symposium and their great work. All errors are my own.

1. *See* John Villasenor, *Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur* (Hoover Inst. Working Grp. on Intellectual Prop., Innovation, and Prosperity, Working Paper No. 14012, 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2488756 (describing the "arms race" between trade secret owners and those who conduct cyberespionage attacks). Plenty of players are on both sides of the equation, particularly governments.

2. *See* David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230, 233–34 (2015) (outlining the threats that U.S. companies face "from those who would hack into their computer systems, including operatives of foreign governments, organized crime syndicates, and various nuisance hackers and thrill-seekers").

3. The United States Department of Homeland Security offers the following "extended definition" of "cybersecurity":

the past few years, the White House has issued several reports on cybersecurity threats against U.S. industry emanating from the Chinese government.[4] The Congressional Research Service (CRS), in a 2014 report to Congress on trade secrecy and federal legislative efforts to address misappropriation, underscores that point by noting the "growing and persistent threat" facing U.S. corporations from "individuals, rival companies, and foreign governments that seek to steal some of their most valuable intangible assets—their trade secrets."[5] Suggesting the breadth of the issue and the scope of legislative proposals, more than twenty bills have been introduced in the 114th Congress purporting to address "data-breach notification, incidents involving other nation-states, information sharing, law enforcement and cybercrime, protection of critical infrastructure

---

> Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

Explore Terms: A Glossary of Common Cybersecurity Terminology, NAT'L INITIATIVE FOR CYBERSECURITY CAREERS & STUDIES, https://niccs.us-cert.gov/glossary (last visited Nov. 15, 2015) (on file with the Washington and Lee Law Review).

4. *See generally Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, EXEC. OFF. OF THE PRESIDENT OF THE U.S. (Feb. 2013), https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf ("This strategy recognizes the crucial role of trade secrets in the U.S. economy and sets out a means for improved coordination within the U.S. government to protect them."); BRIAN T. YEH, CONG. RESEARCH SERV., R43714, PROTECTION OF TRADE SECRETS: OVERVIEW OF CURRENT LAW AND LEGISLATION, (2014), https://www.fas.org/sgp/crs/secrecy/R43714.pdf ("[T]he governments of China and Russia are particularly aggressive and capable collectors of sensitive U.S. economic information and technologies, and Chinese actors are the world's most active and persistent perpetrators of economic espionage." (internal citation and quotations omitted)).

5. Yeh, *supra* note 4, at 1.

(CI), workforce development, and education."[6] Many hearings on cybersecurity have also been held.[7]

Moreover, cybersecurity reporting has become front-page news. Popular magazines like *Consumer Reports* and *Bloomberg Businessweek* have published breathless cover stories proclaiming that "Your Secrets Aren't Safe,"[8] and discussing "The Nasdaq Hack" and the reaction to it that "could destroy your faith in the financial system,"[9] respectively. Recent cyberespionage and intrusions against entities ranging from the U.S. Office of Professional Management[10] to the adultery website Ashley Madison,[11] whose perpetrators have been hard or impossible to identify, have elevated both the hysteria around and the perceived urgency of the problem.[12]

To be sure, there is a major problem in how we approach cybersecurity as a country, and an educated and honest debate of

---

6. RITA TEHAN, CONG. RESEARCH SERV., R43317, CYBERSECURITY: LEGISLATION, HEARINGS, AND EXECUTIVE BRANCH DOCUMENTS 2 (2015), https://www.fas.org/sgp/crs/misc/R43317.pdf.

7. *Id.*

8. *Your Secrets Aren't Safe*, CONSUMER REPORTS (May 2014), http://www.consumerreports.org/cro/magazine/2014/07/your-secrets-aren-t-safe/index.htm (last visited Nov. 21, 2015) (on file with the Washington and Lee Law Review).

9. Michael Riley, *How Russian Hackers Stole the Nasdaq*, BLOOMBERG BUSINESSWEEK (July 17, 2014), http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq (last visited Nov. 21, 2015) (on file with the Washington and Lee Law Review).

10. KRISTIN FINKLEA ET. AL., CONG. RESEARCH SERV., R44111, CYBER INTRUSION INTO U.S. OFFICE OF PERSONNEL MANAGEMENT: IN BRIEF, (2015), https://www.fas.org/sgp/crs/natsec/R44111.pdf.

11. Robert Hackett, *What to Know About the Ashley Madison Hack*, FORTUNE (Aug. 26, 2015), http://fortune.com/2015/08/26/ashley-madison-hack/ (last visited Nov. 21, 2015) (on file with the Washington and Lee Law Review).

12. Indeed, the recent terrorist attacks by the Islamic State have been linked to whistleblower leaks by Edward Snowden, who gained unauthorized access to computer networks from within his contractor post with the National Security Agency. Mathew Blake, *'Isis Are Using Snowden Leaks to Evade US Intelligence': Former NSA Boss Warns Terror Group Are Exploiting Massive Breach of Security*, DAILY MAIL (Sept. 5, 2014), http://www.dailymail.co.uk/news/article-2745010/Isis-using-Snowden-leaks-evade-US-intelligence-Former-NSA-boss-warns-terror-group-exploiting-massive-breach-security.html (last visited Nov. 21, 2015) ("A Senate defense committee staffer said . . . : 'Our lax security has provided our adversaries with a gold mine of information about our tactics and procedures.'") (on file with the Washington and Lee Law Review).

policy options is undoubtedly warranted. The constant struggle to maintain secrets in the face of cyberespionage efforts, foreign and domestic, has appropriately alarmed Congress. Among many other proposals, a new federal trade secret law, dubbed the Defend Trade Secrets Act (DTSA), has been introduced to "stop the hemorrhaging of jobs and revenue being lost to the theft of trade secrets."[13] As explained by its sponsors, "In today's electronic age, trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor."[14] The DTSA's new private cause of action under the existing Economic Espionage Act (EEA)[15] is said to take allegedly "much-needed steps to empower victims of trade secret theft to protect their intellectual property in federal court."[16]

Unfortunately, because the DTSA's sponsors have framed the problem facing U.S. industry as one of insufficient legal recourse in trade secrecy, instead of lax cybersecurity measures, the DTSA is both over- and under-inclusive. It is under-inclusive because it does not directly address acts of cyberespionage, instead requiring proof of the existence of a trade secret as a predicate fact necessary to stop the bad behavior that is the reason behind the legislation. It is over-inclusive because, instead of focusing solely on cyberespionage (in trade secret parlance, "wrongful acquisition"), it would change trade secret doctrine with respect to trade secrets that were rightfully acquired.[17]

---

13. Press Release, Senate, House Leaders Introduce Bipartisan, Bicameral Bill to Protect Trade Secrets (Jul. 29, 2015), http://www.hatch.senate.gov/public/index.cfm/releases?ID=ad28f305-f73a-4529-84ba-ad3285b09d6e [hereinafter Hatch Press Release].

14. *Id.*

15. Defend Trade Secrets Act, S. 1890, 114th Cong. § 2(b) (2015).

16. Hatch Press Release, *supra* note 1313. The professors' 2014 and 2015 letters challenge this assertion. Professors' Letter in Opposition to the "Defend Trade Secrets Act of 2014" ("DTSA of 2014"), S. 2267 (Aug. 22, 2014), http://cyberlaw.stanford.edu/files/blogs/FINAL%20Professors%27%20Letter%20Opposing%20Trade%20Secret%20Legislation.pdf [hereinafter 2014 Professors' Letter]; Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326) (Nov. 4, 2015), https://s3.amazonaws.com/ftt-uploads/2015+Professors+Letter+in+Opposition+to+DTSA+FINAL.pdf [hereinafter 2015 Professors' Letter].

17. *See* 2014 Professors' Letter, *supra* note 16 (explaining in greater detail why the proposed act is over-inclusive); 2015 Professors' Letter, *supra* note 16

Alas, the core problem facing U.S. industry in combating cyberespionage is not a lack of legal remedies,[18] but an inadequate private defense; not a lack of recourse in U.S. courts, but a lack of robust private cybersecurity standards to prevent and detect unauthorized intrusions into computer systems and thefts therefrom. The DTSA's underlying premise is therefore fatally flawed. In fact, the DTSA may actually put more trade secrets at risk of misappropriation as a result.

Compounding the regulatory challenge, the government's role in addressing cybersecurity issues in any context, trade secret misappropriation or otherwise, is far from clear and fraught with risk. Indeed, when Professor Edward Felten of Princeton University, now Deputy Chief Technology Officer of the United States, hypothetically asked in 2004 "what the government . . . can do about private-sector insecurity," he answered that "[c]ertainly, most of the things the government can do would be harmful."[19] More recently, another expert has noted that, given cybersecurity's extreme complexity, "government intervention is a delicate matter that may do more harm than good."[20] Thus, even though cybersecurity is now front-page news,

---

(same).

18. Among the options are existing state trade secret law, contract law, common law trespass to chattels, the CFAA, and the DMCA. James Dowd et. al., *Cyberespionage and Civil Suits*, LAW360 (July 14, 2014); Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2012); Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003); Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2012); Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512 (2012).

19. Ed Felten, *What's the Cybersecurity Czar's Job?*, FREEDOM TO TINKER (Oct. 4, 2004), https://freedom-to-tinker.com/blog/felten/whats-cybersecurity-czars-job/ (last visited Nov. 23, 2015) (on file with the Washington and Lee Law Review).

20. Jeff Williams, *What Government Can (And Can't) Do About Cybersecurity*, DARK READING (Jan. 22, 2015, 10:30 AM), http://www.darkreading.com/risk/what-government-can-(and-cant)-do-about-cybersecurity/a/d-id/1318726 (last visited Nov. 23, 2015) (on file with the Washington and Lee Law Review); *see also* Professors' Letter in Opposition to the "Cybersecurity Information Sharing Act" (S. 754) (Oct. 26, 2015), http://cyberlaw.stanford.edu/blog/2015/04/technologists-oppose-cisainformation-sharing-bills [hereinafter CISA Professors' Letter] (advising that the CISA is not needed for information sharing but will cause privacy and surveillance harms); PAUL ROSENZWEIG, CYBER WARFARE: HOW CONFLICTS IN CYBERSPACE ARE CHALLENGING AMERICA AND CHANGING THE WORLD 162 (2013) ("It turns out that government intervention may do more harm than good–even if it might be theoretically warranted."); Lawrence M. Walsh, *Government Cybersecurity:*

it should be no surprise that it has not been an issue (to date) in the 2016 U.S. Presidential election televised debates. As Steve Morgan, founder and CEO of Cybersecurity Ventures explained to NBC News, "It's a complex topic. It's like quicksand: Once [Presidential candidates] step into it, they're going to sink. They just aren't equipped to talk about it."[21]

Unfortunately, in part due to the rush to act, Congress has often acted in the face of a lack of expertise and ignored experts' warnings. For example, the Cybersecurity Information Sharing Act (CISA), designed to foster sharing about cybersecurity threats, has recently passed over the objections of dozens of security experts.[22] These experts explained that such sharing already occurs and will lead to increased privacy and government surveillance concerns; yet, the law overwhelmingly passed Congress, and the President is expected to sign it into law.[23] Instead of addressing cyberespionage and cybersecurity squarely, Congress has solved a problem that has not been proven to exist, with significant potential downsides.

This Essay argues that the DTSA, if enacted, will become part of that trend. It solves a problem that has not been proven to exist, while creating new or exacerbating existing problems and failing to address cyberespionage directly.[24] Specifically, it argues

---

What is Being Done to Fight Cybercrime?, TECH TARGET (May 1, 2014), http://searchsecurity.techtarget.com/Government-cybersecurity-What-is-being-done-to-fight-cybercrime (last visited Nov. 23, 2015) ("Enterprises fear broad, prescriptive security laws because such laws could actually do more harm than good.") (on file with the Washington and Lee Law Review).

21. Tim Starks, *TPP Text Released*, POLITICO (Nov. 5, 2015, 10:00 AM), http://www.politico.com/tipsheets/morning-cybersecurity/2015/11/new-car-hacking-legislation-set-to-drop-a-dispute-about-a-cisa-dispute-farenthold-cyber-caucus-hit-back-over-asbestos-bill-complaints-211107 (last visited Nov. 23, 2015) (on file with the Washington and Lee Law Review).

22. CISA Professors' Letter, *supra* note 20.

23. *Id.*; Sam Thielman, *Senate Passes Controversial Cybersecurity Bill CISA 74 to 21*, GUARDIAN (Oct. 27, 2015), http://www.theguardian.com/world/2015/oct/27/cisa-cybersecurity-bill-senate-vote (last visited Nov. 23, 2015) (on file with the Washington and Lee Law Review); Jason Koebler, *The Senate Has Overwhelmingly Passed CISA, a Privacy-Killing Cybersecurity Bill*, MOTHERBOARD (Oct. 27, 2015, 4:27 PM), http://motherboard.vice.com/read/the-senate-has-passed-cisa-a-privacy-killing-cybersecurity-bill (last visited Nov. 23, 2015) (on file with the Washington and Lee Law Review).

24. 2014 Professors' Letter, *supra* note 16; 2015 Professors' Letter, *supra*

that rather than addressing the cyberespionage problem, the DTSA would instead provide legal justification for, and therefore help enshrine, the poor corporate cybersecurity practices that are the primary reason why trade secrets are now under such significant threat.

There is a disconnect between the urgent desire for a legislative solution to the cyberespionage problem and the unfortunate reality that legislative solutions are lacking, or at least are exceptionally difficult to craft. Like CISA, the DTSA solves a problem that does not exist—a lack of legal remedies—while failing to address and, in this case, worsening the real problem—a lack of robust cybersecurity. Indeed, better paths to the DTSA sponsors' stated goal exist not in law, but in the marketplace. This Essay is intended to offer a basis for consideration of that better alternative.

As explained by John Villasenor of the Brookings Institution, the "first" and most "obvious" way to address trade secret cyberespionage is for companies to take "all reasonable steps to minimize the ability of cyber-intruders to get into their systems and make off with their trade secrets."[25] This concept arises in—although it is far from identical to—the Uniform Trade Secrets Act's requirement that trade secrets must be "subject of efforts that are reasonable under the circumstances to maintain its secrecy" and can be lost for failure to do so.[26] The DTSA incorporates this requirement.[27] By examining the questionable "reasonable efforts" standard in modern trade secret law, which

---

note 16; Levine & Sandeen, *supra* note 2.

25. Villasenor, *supra* note 1, at 2. These suggestions, it should be noted, are not all technological in their implementation. For example, Villasenor emphasizes the role of the employee, stating that "employees should be . . . encouraged to store and exchange trade secret information only to the extent necessary to do their jobs." *Id.* at 19. Villasenor also makes a second core suggestion. Recognizing that cybersecurity will never be perfect, he recommends that "companies need to manage their intellectual property in light of the affirmative knowledge that their computer systems will sometimes be breached." *Id.*

26. Uniform Trade Secrets Act § 1(4) (amended 1985).

27. The DTSA adopts the EEA definition of a trade secret, which is derived from the UTSA. *Trade Secret*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/trade_secret (last visited Nov. 15, 2015) (on file with the Washington and Lee Law Review); Defend Trade Secrets Act, S. 1890, 114th Cong. § 2(b) (2015).

requires a trade secret owner to take unspecified and ambiguous reasonable efforts to maintain its trade secret,[28] the DTSA's core significant problem comes into stark relief.[29]

To understand this issue, it is helpful to review the facts around, and outcome of, a fateful and famous flight that occurred in March 1969.[30] On that day, Rolfe and Gary Christopher flew in public airspace over an E. I. duPont deNemours & Company ("DuPont") chemical plant that was under construction in Texas.[31] DuPont alleged that the Christophers took photographs of a "highly secret but unpatented process for producing methanol"—in other words, a classic trade secret.[32] Indeed, chemical processes are among the most common forms of trade secrets.[33] They took an alleged sixteen pictures and delivered them to a third party, who to this day remains unknown.[34]

---

28. *See* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1015–16 (5th Cir. 1970) ("To obtain knowledge of a process without spending the time and money to discover it independently is improper unless the holder voluntarily discloses it or fails to take reasonable precautions to ensure its secrecy."). *See generally* Defend Trade Secrets Act, S. 1890, 114th Cong. § 2(b) (2015); Uniform Trade Secrets Act (amended 1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf; Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (2012). *See also* Trans-Pacific Partnership Full Text, Art. 18.78(1), Nov. 5, 2015 (incorporating the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) trade secret definition, which includes the "reasonable efforts" requirement).

29. This Essay is not designed to take on the full ramifications of the reasonable efforts standard. Rather, it is written to illustrate how the DTSA would not make the standard any more robust than it is now, and would rather send U.S. corporations the unfortunate message that the current state of corporate cybersecurity is acceptable, or at least not as significant a Congressional concern as the presumed need for a private federal cause of action under the EEA.

30. *See generally* Robert G. Bone, *Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 46-76 (Rochelle C. Dreyfuss and Katherine J. Strandburg eds. 2011).

31. *E.I. duPont*, 431 F.2d at 1013.

32. *Id.*

33. *See* Aija Leiponen & Justin Byma, *If You Cannot Block, You Better Run: Small Firms, Cooperative Innovation, and Appropriation Strategies*, 38 RESEARCH POL'Y 1478, 1481–83 (2009) (noting that process innovations are usually more effectively protected with trade secrets); Wesley M. Cohen et. al., *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (Or Not)* 6 (Nat'l Bureau of Econ. Res., Working

Logically, DuPont sued for trade secret misappropriation, alleging that the Christophers used "improper means"[35] in acquiring the photographs. As part of its argument, DuPont had to maintain that its efforts to maintain the secrecy of its chemical process were "reasonable"; a key element in the maintenance of a trade secret, then and now.[36] Equally unremarkably, DuPont sought damages arising from the allegedly wrongful action, an injunction against further circulation of the photographs, as well as an order requiring the Christophers to divulge the identity of their employers.

DuPont proved misappropriation, but for a primary reason that sheds light on the panic that has taken hold around cyberespionage and policymaking, a panic reflected in the DTSA. In explaining its holding, the court stated that DuPont had taken "special precautions to safeguard"[37] this trade secret, even though it "was exposed to view from the air."[38] But what do we know of the *actual* efforts to engage in reasonable efforts to maintain the trade secret? We know that DuPont did not put a "roof"[39] over the under-construction plant, and that it did not have—and did not need to have, under trade secret law—an "impenetrable fortress"[40] around the highly secret trade secret. And, from this opinion—which has had a profound effect on trade secret law—that is all we know.

Paper No. 7552, 2000), http://www.nber.org/papers/w7552.pdf ("Secrecy is commonly the dominant mechanism, as in the chemicals industries, semiconductors and others.").

34. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1013 (5th Cir. 1970).

35. *Id.* at 1014. This is also in the modern UTSA. Uniform Trade Secrets Act § 1 (amended 1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

36. *E.I. duPont*, 431 F.2d at 1015–16; *see also Trade Secret*, *supra* note 27 (requiring under the definition of "trade secret" that the item be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy"); Defend Trade Secrets Act, S. 1890, 114th Cong. § 2(b) (2015) (the definition of "trade secret" includes that "the owner thereof has taken reasonable measures to keep such information secret").

37. *E.I. duPont*, 431 F.2d at 1013.

38. *Id.* at 1016.

39. *Id.*

40. *Id.* at 1017.

In a conclusory fashion, the court found that DuPont's efforts were reasonable. The problem, which is also reflected in how the DTSA proposes to address cyberespionage, is that rather than confront the possibility that DuPont could have done more to protect this valuable asset—short of an "impenetrable fortress" but more than seemingly nothing—the court instead focused on the Christophers' spectacular improper means:

> [W]e realize that industrial espionage of the sort here perpetrated has become a popular sport in some segments of our industrial community. However, our devotion to free wheeling industrial competition must not force us into accepting the law of the jungle as the standard of morality expected in our commercial relations . . . . To require DuPont to put a roof over the unfinished plant to guard its secret would impose an enormous expense *to prevent nothing more than a school boy's trick*.[41]

There is an obvious gulf between trade secrecy's standard, reflected in *DuPont*, and Villasenor's practical recommendation that "*all* reasonable steps" must be taken to prevent cyberespionage.[42] Put into modern parlance, the court focused on the defendants' tortious activities rather than what DuPont could have done to prevent theft of its property.

Characterizing the Christophers as engaged in a "school boy's trick" excused the fact that DuPont apparently did little to protect itself from a seemingly obvious, and temporary, vulnerability. Indeed, *DuPont* has been understood by the UTSA's authors to stand for the proposition that "courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage."[43] By following the UTSA/EEA standards in the name of trade secret law "uniformity,"[44] the DTSA similarly excuses substandard cybersecurity against modern misappropriation threats by putting emphasis on the bad acts of U.S. industry's attackers, rather than what U.S. industry should do to prevent that misappropriation in the first place.

---

41. *Id.* at 1016–17 (emphasis added).

42. Villasenor, *supra* note 1, at 2.

43. Uniform Trade Secrets Act § 1 cmt. at 7 (amended 1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf

44. Hatch Press Release, *supra* note 13.

To be sure, the *DuPont* analysis arguably makes sense given the traditional reasons for the reasonable efforts obligation. While the purpose behind the reasonable efforts requirement in trade secret law is unclear,[45] Robert Bone identified the two most prominent traditional arguments for the reasonable efforts requirement as evidentiary[46] and notice.[47] The evidentiary benefit identifies a trade secret owner's reasonable efforts as indicating that a given trade secret has value, while the notice aspect focuses on assuring that the recipient of trade secrets recognizes the secrecy of the information itself. In those ways, the information that must be protected can be identified.

Unfortunately for U.S. industry, school boy tricks have become much more sophisticated and complex since *DuPont*. Obviously, few trade secrets were stored on computers in 1969,

---

45. Indeed, much of trade secrecy's reason d'etre lacks clarity. *See* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 245–46 (1998) ("The reason we have a body of trade secret law with special rules is largely a matter of historical contingency."); Mark A. Lemley, *Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 312 (2008) ("Trade secret law is a puzzle. Courts and scholars have struggled for over a century to figure out why we protect trade secrets. . . . [N]o one can seem to agree where trade secret law comes from or how to fit it into the broader framework of legal doctrine."); Michel Risch, *Why Do We Have Trade Secrets?,* 11 MARQ. INTELL. PROP. L. REV. 1, 3 (2007) ("Trade secrets are curious anomalies in intellectual property law. They are arguably the most important and most litigated form of intellectual property, yet they have recently been called 'parasitic' and the leading economic analysis claims that 'there is no law of trade secrets.'"); Sharon K. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 VA. J.L. & TECH. 1, 38–41 (2014) (providing an outline of trade secret law's history, particularly the ambiguity of the "reasonable efforts" requirement).

46. *See* Bone, *supra* note 30, at 59 (citing Judge Posner for the proposition that "precautions can support a finding of misappropriation because they make lawful acquisition more difficult, and can also support an inference of substantial value because an owner would not invest to protect a secret with little value").

47. *See id.* ("Informing third parties that the owner wishes to preserve secrecy."); *see also* Sandeen, *supra* note 45, at 42–47 (explaining the reasonable efforts requirement and its notice function); Lemley, *supra* note 45, at 348–49 ("[I]t may be that efforts to protect secrecy serve to put potential defendants on notice of the claim of secrecy, and therefore prevent inadvertent misappropriation."); Trygve Meade, *Indecision: The Need to Reform the Reasonable Secrecy Precautions Requirement Under Trade Secret Law*, 37 S. ILL. U. L.J. 717, 724–25 (2013) (outlining the inconsistent application of and reasoning behind the reasonable secrecy precautions requirement).

and the Internet as we know it did not exist.[48] The CRS's report to Congress is framed around technology's developing threat to trade secret protection:

> The tools, tactics, and methods used by [those who seek to steal trade secrets] vary widely but increasingly have involved the use of cyberspace and sophisticated technologies that "mak[e] it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect."[49]

Thus, there is a modern price for *DuPont* and the UTSA's deferential posture in the face of "school boy tricks," namely, that trade secrecy's "reasonable efforts" flexibility downplays the real need for robust and dynamic cybersecurity measures to address the ever-changing challenges to trade secret protection.[50]

We should expect the DTSA to exacerbate this problem. Many trade secret owners, faced with the choice of improving their reasonable efforts to maintain their secrets or suing under the DTSA, will likely choose the latter. Bone explains why this should be expected in his discussion about the ability of the reasonable efforts standard to reduce enforcement "process costs":

> The key to understanding the process cost argument is to recognize that precautions and litigation are substitute methods for protecting a secret. A rational firm with recourse to a trade secret claim will use precautions to protect its secret up to the point where the marginal cost of additional

---

48. *See* Elizabeth A. Rowe, *Rethinking "Reasonable Efforts" to Protect Trade Secrets in a Digital World* 23–27 (Sept. 2008) (unpublished manuscript), http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=elizabeth_rowe (noting that the Internet has made trade secrets more vulnerable).

49. Yeh, *supra* note 4, at 1 (quoting Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, October 2011, at i, http://www.ncix.gov/publications/reports/fecie_all/).

50. Security expert Bruce Schneier also notes that unlike most commercial information that loses value quickly, trade secrets require long-term protection. BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD 61 (2000). Thus, the need for robust cybersecurity in the face of ever-changing cyberintrusion methods and tactics is even more pronounced. *See generally* Rowe, *supra* note 48 (arguing "that the changing circumstances that have come about as a result of new technology requires a reexamination of what security measures are reasonable").

> precaution just exceeds the marginal cost of a trade secret lawsuit and then switch to litigation beyond that point. The problem, of course, is that not all these costs are internalized. . . . Under these circumstances, a rational firm will over-utilize litigation and underutilize precautions because it does not have to pay the full expense of the litigation alternative, including the defendant's litigation costs and the relevant portion of the public subsidy.[51]

Thus, a likely DTSA result will be more lost trade secrets that result in litigation, rather than less trade secret loss from improved cybersecurity in the first instance. Ironically, this is precisely what the DTSA's sponsors are trying to avoid.

By introducing the DTSA, Congress is effectively treating U.S. industry the same way that the Court treated DuPont: as the victim of a tort, a sneaky "school boy's trick" worthy of condemnation, rather than a party with responsibility for protecting its property but nonetheless allowing the "school boy's trick" to cause it such harm. Moreover, by creating a new private trade secret cause of action, Congress is encouraging investment in litigation when investment in better cybersecurity is most needed. While cybersecurity investment across affected industries is expected to increase significantly over the next several years,[52] diversion of limited resources could be the difference between a successful cyberintrusion versus one that is contained or avoided.

This misplaced priority seems to extend to the Department of Justice, if the recently unsealed criminal complaint in *United States v. Zeng*[53] is any indication. *Zeng* is a criminal action for trade secret misappropriation under the Electronic Espionage

---

51. Bone, *supra* note 30, at 67–68. *See also* David D. Friedman, William Landes & Richard A. Posner, *Some Economics of Trade Secret Law*, 5 J. ECON. PERSPECTIVES 61, 68 (1991) ("Even if there is no law against theft of trade secrets, there is plenty a firm can do to reduce the probability of such thefts (screening employees more carefully, installing more effective security systems, and so forth); it will do less if the threat of legal sanctions deters." (citation omitted)).

52. *See Cyber Security Investing Grows, Resilient to Market Turmoil*, REUTERS (Sept. 23, 2015), http://fortune.com/2015/09/23/cyber-security-investing/ (last visited Nov. 23, 2015) ("[W]orldwide spending on information security technology is expected to grow from about $77 billion this year to $108 billion in 2019 . . . .") (on file with the Washington and Lee Law Review).

53. No. 3-15-71060 (N.D. Calif. Aug. 20, 2015).

Act.[54] The defendant, Jing Zeng, was an employee of Machine Zone, Inc., developer of the Internet videogame "Game of War."[55] According to the complaint, on July 8, 2015, Zeng was informed by Machine Zone that he would be "exiting" the company.[56]

What happened after that date underscores Machine Zone's arguable lack of reasonable efforts taken to protect its alleged trade secrets. *After* that date, Zeng repeatedly downloaded alleged trade secrets for which he had "no business reason."[57] *After* a July 10 meeting with Machine Zone senior employees where Zeng noted that his termination was "unfair" and "made statements . . . interpreted as threatening to the company,"[58] he was allowed to leave Machine Zone's office with his company laptop.[59]

Zeng later admitted that he had "downloaded files from the company-issued laptop, backed up the files to a USB drive or a larger portable external hard drive, and later wiped [i.e., erased] the laptop during a drunken moment."[60] Indeed, Zeng apparently copied "certain Machine Zone files and documents onto his laptop from an external device" at 10:00 AM on July 15.[61] He returned the company laptop to Machine Zone thirty minutes later—five days after he had threatened Machine Zone and one day after he was asked to return the laptop.[62] Some of the storage devices wound up in China, prompting the criminal complaint.[63]

---

54. Complaint ¶ 1, United States v. Zeng, No. 3-15-71060 (N.D. Calif. Aug. 20, 2015). It should be noted that a stated justification for the EEA is that the Department of Justice lacks the resources to bring EEA actions, so the private sector must be empowered to vindicate these rights. Hatch Press Release, *supra* note 13. While it is one case, the *Zeng* prosecution suggests that further study is warranted to provide evidence for this assertion.

55. Complaint ¶ 2, United States v. Zeng, No. 3-15-71060 (N.D. Calif. Aug. 20, 2015).

56. *Id.* ¶ 28.

57. *Id.* ¶¶ 28–31, 41.

58. *Id.* ¶ 32.

59. *Id.* ¶ 34. His access to Machine Zone's computer system was apparently shut off at 4:00 PM that day. *Id.*

60. *Id.* ¶ 52.

61. *Id.* ¶ 39.

62. *Id.*

63. *Id.*

Machine Zone's actions arguably fail the "reasonable efforts" standard. Far from being a cyberintrusion from the outside, Machine Zone was primarily victimized in trade secrecy's typical way, from within. By failing to exercise basic common sense, like not allowing a threatening employee access to trade secrets and letting him leave Machine Zone's offices with a company laptop after he had made such threats, Machine Zone allowed its trade secrets to be compromised.[64] *Zeng*'s seeming obliviousness to Machine Zone's cybersecurity shortcomings underscores the need to consider the potential palliative effects of criminal prosecutions—and a new private federal cause of action—on current lackluster cybersecurity practices and standards. The simple fact is that Machine Zone had the power and ability to engage in self-help efforts, but failed to do so.

To be sure, not all courts are sympathetic to trade secret owners who fail to meet the minimal reasonable efforts burden in existing trade secret law. Robert Bone explained a few of these cases:

> One court explained that a trade secret owner who "disregards caution" is denied relief "on the theory that he courted his own disaster," perhaps suggesting an assumption of risk rationale. Another drew a connection to the clean hands doctrine in equity: "To put it another way, the employer must come into court with clean hands; the employer cannot complain of the employee's use of information if the employer has never treated the information as secret." And yet another court simply asserted without additional argument, but perhaps with the idea in mind that self-help might be less costly than litigation, that "it would be anomalous for the courts to prohibit the use of information that the rightful owner did not undertake to protect."[65]

---

64. *See, e.g.*, *Protecting Trade Secrets When Employees Depart*, LAW360 (Sept. 18, 2009, 11:16 AM), http://www.law360.com/articles/116377/protecting-trade-secrets-when-employees-depart (last visited Nov. 23, 2015) ("Once the employer is aware that an employee is leaving, steps should be put in place to limit or eliminate that employee's access to the company's trade secrets and confidential information. This might include changing passwords, requiring the return of laptop computers and handheld devices, and eliminating remote access.") (on file with the Washington and Lee Law Review).

65. Bone, *supra* note 30, at 60–61 (quoting RTE Corp. v. Coatings, Inc., 267 N.W.2d 226, 233 (Wis. 1978); Electro-Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (Minn. 1983); Dicks v. Jensen, 172 Vt. 43, 50 (2001)).

More recently, some courts have taken notice of poor cybersecurity as a basis to deny trade secret protection because of a failure to exercise reasonable efforts.[66] Nonetheless, the DTSA's focus on litigation against bad actors obscures the fact that reasonable efforts to maintain trade secrets are the first line of defense against misappropriation, not the second.

Perhaps it is time for Congress to focus more on the question of what responsibility U.S. industry has to engage in self-help, and less on the tricks that it has to ignominiously face. It may be time to take "reasonable efforts" more seriously, or redefine its meaning in a cybersecurity context.[67] Perhaps we should consider adopting a more robust and specific "reasonable cybersecurity"

---

66. *See* Wayman Fire Protection, Inc. v. Premium Fire & Security, LLC, No. 7866-VCP, 2014 WL 897223, at *16 (Del. Ch. Mar. 5, 2014) (finding that simply relying on primarily a password requirement was insufficient to show reasonable efforts); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1334–35 (N.D. Ga. 2007) (finding a lack of reasonable efforts to maintain secrecy where plaintiff failed to show that it labeled the file confidential or otherwise communicated the confidentiality of the file to its employees, directed its employees to maintain the secrecy of the file, or tracked or otherwise regulated the use of the file); Boston Laser, Inc. v. Zu, No. 3:07-CV-0791, 2007 WL 2973663, at *10, *12 (N.D.N.Y. Sept. 21, 2007) (finding that the plaintiff had not taken reasonable measures to preserve secrecy where, among other things, "the computer network on which such matters are digitally stored is generally not even password protected beyond the log-in process"); PatientPoint Network Solutions, LLC v. Contextmedia, Inc., No. 1:14-CV-226, 2014 WL 1152940, at *8 (S.D. Ohio Mar. 21, 2014) (finding that the plaintiff's failure to make a written demand for the return of employee's company-issued laptop and iPad upon termination, the plaintiff's failure to request that the employee return other purportedly proprietary and trade secret information, and the plaintiff's waiting six months after it discharged the former employee before making a written demand for the return of these items and information did not amount to reasonable efforts).

67. While beyond the scope of this Article, Villasenor has identified five recommendations for improved cybersecurity to protect trade secrets: (1) Companies Should Segment Their Networks and the Trade Secret Information on Those Networks; (2) Companies Should Avoid Overreliance on NDAs on Mechanisms to Protect Trade Secrets Because Over-Disclosure Can Lead to Increased Exposure to Cyber-Enabled Trade Secret Theft; (3) Companies Should Act More Quickly on Patentable Inventions; (4) Companies Should Ensure That Cybersecurity Considerations Are Part of Their Patent and Trade Secret Decisions; (5) For Inventions Retained as Trade Secrets, Early Commercial Use Can Provide Important Protection if the Trade Secret is Later Patented by a Third Party. Villasenor, *supra* note 1; *see also* Rowe, *supra* note 48, at 15–28 (explaining how technological advances can increase challenges to companies' data security and trade secret protection).

standard rather than "reasonable measures" in the abstract, or tailor it to particular types of threats.

Importantly, this article does not argue for a more robust codified reasonable efforts standard *per se*, but rather highlights the importance of applying the existing requirement appropriately to ensure that U.S. trade secret owners take responsibility for their own cybersecurity. There are potential downsides to a more rigorous application of the reasonable efforts requirement, including the potential for less diffusion of information and some bad actors walking away from bad acts.[68] But these concerns should be weighed against the costs to be incurred if the reasonable efforts requirement is effectively ignored because the defendant's activities are deemed to be egregious. Those issues are worthy of deeper analysis than can be considered in this article. But that's the point: The fact that this issue requires much more analysis and thought underscores the need to reject the DTSA.[69]

Especially given the lack of understanding and empirical evidence as to the potential impact of a massive change in U.S. trade secret law, the DTSA should be abandoned.[70] The DTSA has not been thoroughly vetted, and its potential to create worse

---

68. *See* Bone, *supra* note 30, at 21 ("[R]estricts diffusion by encouraging trade secret owners to bolster their self-help measures."); *see also* Lemley, *supra* note 45, at 348–49 (noting potential negative effects that could stem from heightened reasonable efforts requirements). *See generally* David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135 (2007) (explaining how the aims of secrecy sometimes conflict with "the methods and purpose of transparent and accountable democratic governance").

69. *See* Hatch Press Release, *supra* note 13 (admitting the complexities of trade secret law in light of endless technological advancements). The fact of uniformity is also in dispute. *See* 2014 Professors' Letters, *supra* note 16 (arguing that "[t]he Acts will damage trade secret law and jurisprudence by weakening uniformity while simultaneously creating parallel, redundant and/or damaging law"); 2015 Professors' Letters, *supra* note 16 (same).

70. As a general matter, trade secret law suffers from a severe lack of empirical research. *See* David Almeling et. al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZAGA L. REV 291, 295 (2009/2010) ("In contrast to patents, trademarks and copyrights, little statistical analysis exists on either trade secrets or trade secret litigation. For trade secrets, the explanation is simple - because trade secrets must be kept secret to qualify for protection, there is little publicly available material to study.") Thus, the DTSA is a massive and very risky experiment with little relevant evidence to support it.

conditions for U.S. industry is real. We must reconsider whether we want to treat today's sophisticated foreign cyberespionage the same way as we have treated yesterday's "school boy's trick." Due to the fact that trade secrets cease to exist once they are publicly disclosed, it is better that trade secret information never be wrongful acquired, disclosed, or used in the first place. Therefore, U.S. industry would do well to focus its efforts on improved cybersecurity to prevent or contain trade secret losses, rather than litigation around the damage arising from its loss.