Florida Law Review

Volume 59 | Issue 1 Article 2

January 2022

Secrecy and Unaccountability: Trade Secrets in our Public Infrastructure

David S. Levine

SECRECY AND UNACCOUNTABILITY: TRADE SECRETS IN OUR PUBLIC INFRASTRUCTURE

David S. Levine[*]

Abstract

Trade secrecy—the intellectual property doctrine that allows businesses to keep commercially valuable information secret for a potentially unlimited amount of time—is increasingly intruding in the operation of our public infrastructure, including voting machines, the Internet, and telecommunications. A growing amount of public infrastructure is being provided by private entities that are holding critical information about their goods and services secret from the public. This Article examines this phenomenon, which is largely unexplored in legal scholarship, and identifies a significant conflict between the values and policies of trade secrecy doctrine and the democratic values of accountability and transparency that have traditionally been present in public infrastructure projects.

This Article argues that trade secrecy must give way to traditional notions of transparency and accountability when it comes to the provision of public infrastructure. Although there are good reasons for trade secrecy in private commerce, when applied to public infrastructure, the basic democratic values of transparency and accountability should prevail. The application of trade secrecy doctrine to public infrastructure projects causes some unanticipated outcomes, like hiding information that could be useful for both the public at large and for the improvement of the specific infrastructure project at issue. This Article examines the background and history of trade secrecy and contrasts its values with those of democratic government. It then shows the increasing impact of trade secrecy on public infrastructure through three examples. Finally, the Article suggests some potential remedies to this sphere of increasingly conflicting values.

---

* Resident Fellow at Stanford Law School's Center for Internet and Society (CIS). I thank Bodo Balasz, John Barton, Marilee Chan, Colleen Chien, Benjamin Costa, Jonathan Entin, Paul Goldstein, Tait Graves, Raymond Ku, Mark Lemley, Lawrence Lessig, Jacqueline Lipton, Kevin McMunigal, Craig Nard, David Olson, David Quast, Sharon Sandeen, Chris Sprigman, Jayashri Srikantiah, Steven Star, and Tim Wu for their time, input and thoughtful comments. I am also grateful for the comments received from participants at the University of Pittsburgh Works-in-Progress Intellectual Property Colloquium, a talk at Southwestern School of Law, and the Speaker Series at CIS. For research support in tracking down hard-to-find articles, I thank George Wilson and Sonia Moss of the Stanford Law Library.

I. INTRODUCTION

Trade secrecy, by its very name, invokes two core interests: secrecy and commerce. It is a singularly commercial doctrine designed to protect commercial interests by allowing companies and individuals to keep secret, for a potentially unlimited time, those formulas, processes, and

inventions that afford them pecuniary gain.[1] Standing in stark contrast to those methods and goals, the ideals, if not the daily practice, of democratic government minimize commercial interests and generally abhor secrecy as a default position.[2] Transparency and accountability, especially in the last several decades, are among the core values that drive the fundamental model of a publicly elected and properly operating democratic government.

There has always been tension between the interests of the public and commerce. Indeed, Cato fought the aversion of many of his contemporaries against the involvement of private persons in the functioning of government.[3] But those observing governmental operations, in the intervening millennia, would now regard Cato's position as received wisdom. The public and private sector do not operate without regard for the operations or interests of the other; rather, they increasingly can and do regard the other as a direct partner in achieving their vastly different goals. Increasingly, this intersection of the private person and government is causing doctrinal conflicts in the rules that have governed these two areas.

Fixed at the intersection of these increasingly intertwined worlds is trade secret law. Private businesses are increasingly displacing the government in providing and operating public infrastructure, but these private businesses are utilizing commercial law standards and norms, including the key tool of trade secrecy, to do so. Countless examples of modern infrastructure, from telecommunications in the form of the Internet, to traditional government operations in the form of voting machines, are now being provided by the private sector. Because of this shift to private provision of public infrastructure, the trade secrecy doctrine has intruded into activities that traditionally have been conducted in the relatively open realm of public institutions like government. I argue in this Article that public access to information should prevail over trade secrecy protection in this sphere.[4]

---

1. The seminal definition of trade secrets found in the RESTATEMENT (FIRST) OF TORTS states, "A trade secret may consist of any formula, pattern, device, or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939). This definition has changed and expanded over time. *See infra* Part III.B.

2. *See infra* note 96.

3. "'Some have said that it is not the business of private men to meddle with government—a bold and dishonest saying, which is fit to come from no mouth but that of a tyrant or a slave. To say that private men have nothing to do with government is to say that private men have nothing to do with their own happiness or misery; that people ought not to concern themselves whether they be naked or clothed, fed or starved, deceived or instructed, protected or destroyed.'" Cato, *Introductory quotation* to STUART CLOETE, THE THIRD WAY (1947).

4. The application of trade secrecy to the private provision of public infrastructure, discussed in this Article, remains largely unexplored in law literature. Indeed, trade secrecy itself is under-explored and under-analyzed in legal scholarship. For discussions of related issues see, for

Secrecy, and its attendant goals of pecuniary gain and commercial competition, conflict with the methods and purpose of transparent and accountable democratic governance. This conflict is crystallized in the private distribution of voting machines. Voting machines are perhaps the signature example of a device designed to advance governmental and democratic interests. Diebold Election Systems, Inc. (Diebold), by its own estimation, is currently providing over 130,000 voting machines to states.[5] These machines, replacing older (but not necessarily less reliable) pull-lever and punch-card systems, are the public infrastructure through which elections are conducted, votes are counted, and the results are verified. They form the backbone upon which one can exercise the right to vote; they instill confidence that one's vote will not be disregarded, lost, or erroneously tabulated.

As examined below, however, public access to the internal workings of these machines is difficult, or in some cases impossible, to obtain. North Carolina's experience with Diebold illustrates this problem. The North Carolina State Board of Elections, charged by statute to procure voting machines for use in its elections, is legally required to have access to the inner workings of potential vendors' machines. This requirement exists to guarantee that the Board meets its responsibilities to conduct error-free and fraud-free elections, and that the vendors supply the information.[6] The disclosure of this information helps to provide legitimacy to, and trustworthiness in, the very system of conducting elections—a bedrock requirement of a transparent democratic society.

But in late 2005, potential vendor Diebold, when faced with this law's requirements, responded differently and focused instead on its commercial property rights. Rather than comply with the law, it brought a declaratory judgment action against the state, arguing that it could not supply the required information.[7] Diebold explained that some of the inner workings of its voting machines were a third party's intellectual property, likely trade secrets, to which it did not have access.[8] Therefore, Diebold claimed the information could not be shared with the state or the public without violating intellectual property rights or intellectual property licensing agreements with third parties, even if it had access to this information.

---

example, Sharon K. Sandeen, *Preserving the Public Trust in State-Owned Intellectual Property: A Recommendation for Legislative Action*, 32 MCGEORGE L. REV. 385, 386, 387 (2001) (discussing the ownership of intellectual property by governments); Michael P. Simpson, Note, *Future of Innovation Trade Secrets, Property Rights, and Protectionism—an Age-Old Tale*, 70 BROOK. L. REV. 1121, 1122 (2005) (discussing the trend towards favoring restrictive trade secret protection over cooperative innovation and suggesting potential solutions to the posed problem).

5. Diebold Election Systems, About Diebold Election Systems, http://www.diebold.com/dieboldes/ (last visited Nov. 13, 2006).

6. *See infra* note 199 and accompanying text.

7. *See infra* note 200 and accompanying text.

8. *See infra* note 201 and accompanying text.

Was this a legitimate objection based upon Diebold's trade secret rights? From a business perspective, it would appear so; but exercising those rights frustrated the goals of public transparency and accountability. Rather than comply with the law, Diebold chose to keep its secrets and withdraw from competition for the state's contract.[9]

The Diebold story is one of many. Today, more and more public infrastructure is provided by the private sector while the use of trade secrecy by the business world is expanding. Despite the relative dearth of scholarly analysis of trade secrecy, as compared to copyright and patent law, it is a vitally important business practice. For example, in one empirical study of 1,478 manufacturing firms, secrecy ranked first or second in importance for product innovations in twenty-four of the thirty-three surveyed industries.[10] Significantly, secrecy was generally emphasized over both patents and lead-time in the development of new processes.[11] Indeed, one study concluded that between the early 1980s and the mid-1990s the use of secrecy to protect product innovations had "increased dramatically."[12] Even in Silicon Valley, the center of the technology world, the use of trade secrecy to maintain a "competitive edge" has been on the rise.[13] Thus, the use of secrecy as a core business tool is increasing in use and importance.[14]

The detrimental effects on access to information grow as private industry increasingly relies on secrecy to achieve its goals, while, at the same time, the breadth of application of the trade secrecy doctrine continues to expand. Should we want or expect private companies like Diebold to adhere to public values like transparency and accountability in the provision of public infrastructure, and, if so, can this goal be achieved

9. *See infra* note 205 and accompanying text.

10. Wesley M. Cohen et al., *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (Or Not)* 13 (Nat'l Bureau of Econ. Research, Working Paper No. 7552, 2000), *available at* http://www.nber.org/papers/w7552.pdf.

11. *Id.* at 10.

12. *Id.* at 3.

13. *See* Hanna Bui-Eve, *To Hire or Not to Hire: What Silicon Valley Companies Should Know About Hiring Competitors' Employees*, 48 HASTINGS L.J. 981, 993 (1997) (noting this trend).

14. *See* 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"); Josh Lerner, The Choice of Intellectual Property Protection: Evidence in Civil Litigation 1 (1994) (unpublished manuscript, on file with author) (analyzing the importance of certain intellectual property protections for 530 manufacturing firms based in Middlesex County, Massachusetts, and noting that "cases involving informal protection—through the mechanism of trade secrecy rather than patents, trademarks or copyrights—are commonplace, figuring in 43% of the intellectual property disputes."). To that end, the overuse and improper assertion of trade secrecy protection should be a concern.

under the current trade secrecy framework?[15] I argue here that we can and should expect such public disclosure when companies step out of the purely private commercial world and seek to reap the financial benefits of providing essential public infrastructure, and that trade secret law stands in the way of this goal.

The people and the government, in these contexts, are not simply buying a product or service where the product legitimately incorporates trade secrets. Rather, the products or services being procured—and their attendant trade secrets—are themselves the public infrastructure that people have traditionally turned to a publicly accountable government to provide, like the ability to vote, communicate, and access governmental services. If we do nothing, it will be the infrastructure itself—owned and operated by private interests with commercial values like business advantage and secrecy of corporate information—that will direct the law involving public activity, rather than the law creating the conditions under which public infrastructure operates.

Trade secrecy law and practices serve many useful and important purposes in private industry, but, as I argue here, their use in the public infrastructure context is inappropriate, unexpectedly powerful, and doctrinally unsound. When private firms provide public infrastructure, commercial trade secrecy should be discarded (at least in its pure form) and give way to more transparency and accountability. Industry's broad definition of "trade secrets," derived from trade secrecy theory, caselaw, and statutes, is inapplicable to a transparent democratic society.

While the public's interest should prevail, there are certain benefits to business that may lessen the sting of the loss of trade secrecy protection. A lack of knowledge about the operations of public infrastructure—and industry's efforts to keep such knowledge from the public—creates an atmosphere of concern and lack of trust between industry and the public, especially in a society infused with fears about national security. By utilizing a commercial doctrine like trade secrecy while at the same time requiring that the public use private industry's services for day-to-day activities, concern, resentment, and distrust exist that might be significantly lessened were trade secrecy limited.

This Article will examine the problem by first outlining and defining "public infrastructures" that now rely on private industry for their maintenance. Part III of this Article traces the relevant history and theoretical underpinnings of trade secrecy law, including secrecy, commercial use, and fair competition. Part IV contrasts this framework with two core modern democratic principles, transparency and accountability. Additionally, Part IV develops the conflict between these

15. Others have made the argument that publicly funded research should not result in trade secrecy. For a thorough discussion of this issue see Sandeen, *supra* note 4, at 401.

competing doctrines and the ramifications of this conflict. Part V analyzes several recent examples of this problem in the United States, including Diebold's. I identify the undemocratic results that can occur and the lessons that can be learned from these events. Part VI considers potential solutions, including the complete abandonment of trade secrecy in the public infrastructure context and less drastic measures such as a durational limit on trade secrecy protection, limitations of remedies for misappropriating a public infrastructure trade secret, or simple money damages. I conclude that the best solution is the complete abandonment of trade secrecy in the private provision of public infrastructure.

II. DEFINING PUBLIC INFRASTRUCTURE AND RECENT TRENDS

This Article examines the growing private provision of public infrastructure. For purposes of this Article, I define public infrastructure as essential goods and services drawn from the set of public works traditionally supported or directed by the public sector, including the operations of the government itself.[16] This definition includes such categories as telecommunications, governmental operations, and energy.[17] Indeed, this definition is broad enough to include many areas in which trade secret law interacts with the private provision of public goods and services.

It is important to note the limited definition employed in this Article. As Professor Brett Frischmann has noted in his extensive studies of commons, the word "infrastructure" usually "conjures up the notion of physical resource systems made by humans for public consumption," like roads, telephone networks, courts, and schools.[18] Frischmann defines these types of infrastructure as "traditional."[19] My focus is on those traditional forms of essential infrastructure that have generally been the domain and responsibility of government to provide, or at least regulate.

The involvement of private industry in the provision of this traditional public infrastructure, which runs the gamut from roads to waste treatment facilities, is rapidly increasing in the United States, as well as Europe and South America.[20] In most parts of the world, the public sector is now

16. I adopt this definition, with revision, from a definition of infrastructure found in William F. Fox & Sanela Porca, *Investing in Rural Infrastructure*, *in* BEYOND AGRICULTURE: NEW POLICIES FOR RURAL AMERICA 63, 63 (Mark Drabenstott ed., 2000), *available at* http://www.kc.frb.org/PUBLICAT/beyond/RC00Fox.pdf. This definition suggests the related question of what public infrastructure information should be made public versus kept secret. While discussed herein, a full examination of this question is beyond the scope of this Article. *See infra* note 154 and accompanying text.

17. *See id.*

18. Brett M. Frischmann, *Infrastructure Commons*, 2005 MICH. ST. L. REV. 121, 123 (2005).

19. *Id.*

20. SIDNEY M. LEVY, BUILD, OPERATE, TRANSFER: PAVING THE WAY FOR TOMORROW'S

viewed as incapable of providing and maintaining infrastructure, and, combined with the need to keep taxes down, the result is an ever-increasing amount of public infrastructure in the hands of private entities.[21] Indeed, current privatization proposals include "privatizing services which, in some countries, have historically been considered to be largely, sometimes almost exclusively, the domain of the public sector," like waste disposal and prisons.[22]

Additionally, the government's share of research and development dollars in the United States has fallen from 67% in 1960 to 26% in 2000, indicating this greater reliance on the private sector for the development and provision of public infrastructure.[23] The result: "Instead of driving

---

INFRASTRUCTURE 8 (1996). By way of a few recent domestic examples, New York Governor George E. Pataki is considering selling the Tappan Zee Bridge to private companies in order for the bridge to be refurbished, rebuilt, or both. Patrick McGeehan, *A Bridge That Has Nowhere Left to Go*, N.Y. TIMES, Jan. 17, 2006, at B1. Similarly, the state of Indiana has considered the approval of a lease of the 157-mile Indiana Toll Road, known as the "Main Street of the Midwest," to a Spanish-Australian consortium that would operate the road for the next seventy-five years. Rick Callahan, *Cash-Strapped States Eye Tollway Leases*, BOSTON.COM, Feb. 1, 2006, http://www.boston.com/news/nation/articles/2006/02/01/cash-strapped_states_states_eye_tolling_leases/?rss_id=Boston.com. The consortium would pay the state to police the road, but would otherwise be responsible for its maintenance, upkeep, and operation, while at the same time reaping the profits. *Id.* Illustrating how governments rely on private-sector technical providers, the state of Rhode Island's website, http://www.ri.gov, operated by the private company New England Interactive, reported a security breach in the website whereby over 4,000 credit card numbers were stolen. Ray Henry, *Credit Card Info May Be Vulnerable*, RUTLAND HERALD, Jan. 28, 2006, http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20060128/NEWS/601280337. The state apparently relied on the private provider to fix the problem and report the breach to the relevant law enforcement and financial institutions. *See* Security Breach-FAQ, Rhode Island Government, http://www.ri.gov/security (last visited Oct. 16, 2006). In a telling scenario, for several days hundreds of automobiles were trapped in a parking garage owned by the City of Hoboken, New Jersey, when the employees of the company that owned the software that operated the Robotic Parking "fully automated parking structure[]" were booted by the City during a contractual dispute. Quinn Norton, *Giant Robot Imprisons Parked Cars*, WIRED NEWS, Aug. 8, 2006, http://www.wired.com/news/technology/1,71554-0.html. The Robotic Parking employees took with them the "intellectual property rights to the software that made the giant robotic parking structure work." *Id.* The City eventually settled, agreeing to pay a $5,500 per month fee to Robotics for a three-year license to operate the software. *Id.*

21. A.J. SMITH, PRIVATIZED INFRASTRUCTURE: THE ROLE OF GOVERNMENT 4 (1999). Indeed, Portland's recent efforts to create a citywide fiber network for Internet access has met with some concern regarding how it will be financed. Aliza Earnshaw, *City's Fiber Plan Could Face Opposition From Telecoms*, PORTLAND BUS. J., Feb. 3, 2006, *available at* http://www.bizjournals.com/industries/high_tech/internet/2006/02/06/portland_story5.html. Quipped one observer, "I don't think the city has $470 million laying around." *Id.* As a result, the financing considerations are limited to creating a public-private partnership, or simply asking a private company to build and own the network. *Id.* The provision of citywide Internet access is an illustrative scenario. *See infra* Part V.

22. SMITH, *supra* note 21, at 5.

23. U.S. GEN. ACCOUNTING OFFICE, INDUSTRY AND AGENCY CONCERNS OVER INTELLECTUAL PROPERTY RIGHTS 1 (2002) (providing the statement of Jack L. Brock, Jr.,

research and its outcomes, the government must increasingly rely on the commercial sector."[24] Thus, industry's increasing reliance on trade secrecy and its increasing involvement and influence in public infrastructure brings the values of trade secrecy and democratic government in conflict.

Moreover, one critical component of public infrastructure, the Internet, is operated by the private sector. Today, for example, backbone functionality—the communication system that allows information to be transferred from one computer to another—is provided entirely by the private sector.[25] Given that it is in private hands, the rapidly expanding use of this computer technology in the operations of varying forms of public infrastructure raises concerns.

Furthermore, the capabilities of infrastructure are increasing because of the use of information technology, like the Internet. Information technology has enabled infrastructure to expand both its geographical scope and its capabilities.[26] Its impact is seen from the management of the flow of traffic on roads to the day-to-day operations of local government.[27] Computer networks are fundamental to the operations of such public infrastructure as transportation, water supply, power, and emergency services; without functioning computer systems, they would stop working.[28] Thus, it is difficult to underestimate the reliance that we now place on technology provided by private entities for the operation of public infrastructure.[29]

Additionally, and more broadly, society increasingly uses public infrastructure. It is omnipresent in all aspects of our lives, from walking

---

Managing Director, Acquisition and Sourcing Management).

24. *Id.*

25. *See* Viktor Mayer-Schoenberger & Gernot Brodnig, *Information Power: International Affairs in the Cyber Age* 23 (Kennedy Sch. of Gov't, Harvard Univ., Faculty Research Working Paper Series, 2001), *available at* http://ksgnotes1.harvard.edu/Research/WPaper.nsf/ (follow "By Author" hyperlink; then follow "Mayer-Schoenberger" hyperlink).

26. Rae Zimmerman & Thomas Horan, *What are Digital Infrastructures?*, *in* DIGITAL INFRASTRUCTURES 3 (Rae Zimmerman ed., 2004).

27. *Id.*

28. Mark G. Milone, *Hacktivism: Securing the National Infrastructure*, 58 BUS. LAW. 383, 383 (2002).

29. Individuals are also impacted when computer networks fail. For an individual user, when the Internet's "backbone" companies stop providing service or simply have interruptions, the effect is substantial. *See* John Borland, *Blackout Shows Net's Fragility*, CNETNEWS.COM, June 6, 2006, http://news.com.com/2102-1038_3-5890424.html?tag=st.util.print (reporting on a feud between two rival backbone Internet companies that resulted in perhaps millions of people being unable to access portions of the Internet when one company cut off direct communications with the other). When this happens millions of users can be cut off from vast swaths of the Internet. *See id.*; Tom Sanders, *Web Outage Hits 120,000 Websites*, VNUNET.COM, Nov. 29, 2005, http://www.vnunet.com/articles/print/2146835 (reporting on a hardware malfunction at domain name provider Network Solutions that resulted in 120,000 websites being unreachable for over one hour).

down the street to being able to contact emergency services if the need arises. As such, it provides the basic conditions for people to live and for businesses to exist; its failure is considered one of today's major security vulnerabilities.[30] Professor Mark Lemley has noted that the "market economy would grind to a halt without the constant support provided by roads, bridges, airports, and the other infrastructure of modern government."[31] Tellingly, a recent report by the Center for Strategic and International Studies found that "[d]emand for infrastructure services is outpacing maintenance, renovation, and construction of new facilities in many infrastructure modes," including mass transit, freight tonnage, and roadways.[32] As private industry provides more and more of this infrastructure, the urgent need to examine how it does business is obvious. Trade secrecy is one such tool of business, and its use warrants this exploration.

In sum, the particular convergence of the increased use of technology in the operation and provision of public infrastructure, combined with public infrastructure's increased importance in our daily lives, makes the issue of the imposition of trade secrecy in public infrastructure all the more important. The technology industry's involvement in the provision of public infrastructure, and how the use of trade secrecy impacts the public, are instructive examples of the values in conflict.[33] Reconsidering how trade secrecy applies in the context of public infrastructure generally, and explaining specific examples of its application by private technology

30. P.M. Herder & W. A. H. Thissen, *Critical Infrastructures: A New and Challenging Research Field, in* CRITICAL INFRASTRUCTURES: STATE OF THE ART IN RESEARCH AND APPLICATION 1 (Wil A. H. Thissen & Paulien M. Herder eds., 2003).

31. Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 533 (2003).

32. EVERETT EHRLICH, PUBLIC WORKS, PUBLIC WEALTH: NEW DIRECTIONS FOR AMERICA'S INFRASTRUCTURE 3-4 (2005) (noting that infrastructure is a "central part of [the United States'] economic life").

33. Much has been written on the particular reasons and conditions that have led to the rapid development over the last thirty years of Silicon Valley in California, versus the Route 128 corridor in Massachusetts. *See, e.g.*, ANNALEE SAXENIAN, REGIONAL ADVANTAGE 1-2 (1996) (comparing and contrasting the two regions). While there are many aspects to this development, one interesting fact, as noted and explored in Saxenian's excellent book, is that the sharing of information and the free movement of employees (and their knowledge) from one employer to another helped lead to Silicon Valley becoming the center of the technology world by the mid-1990s. *Id.* at 34-37. Secrecy was far less utilized in Silicon Valley than in Massachusetts; "collective learning" was a focus in Silicon Valley in a way that did not exist in Massachusetts. *Id.* at 2-4, 36-37, 71-73, 149; *see also* Ronald J. 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, 620 (1999) (explaining that California voids "employer-imposed restraints on employee mobility," thereby encouraging "knowledge spillovers," whereas Massachusetts enforces such restraints, thereby blocking such spillovers); Tait Graves & Alexander Macgillivray, *Combination Trade Secrets and the Logic of Intellectual Property*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 261, 274 (2004) (noting that "scholars have found that states with a less overbearing trade secrets regime are more likely to provide for growth in high-technology industry").

companies, can serve as a useful model to reconsider trade secret applicability in this critical aspect of public life.

III. THE POLICIES AND VALUES OF TRADE SECRET LAW

At its core, trade secret law envisions a fundamental scenario: competition between private actors whose primary objective is pecuniary gain.[34] As previously noted, the most often-cited definition of trade secrets, found in the Restatement (First) of Torts, states: "A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[35] Thus, it is fair to summarize the general qualifications for having a trade secret as information that: (1) confers some sort of competitive advantage, (2) when secrecy is maintained, and (3) is not in the public domain or otherwise publicly known.[36] Each element will be explored below, as their contours are not as obvious as may appear.

As broad as this definition is—including within its grasp all manner of business information and cited often to this day as the basic definition of a trade secret—it has been expanded even further over the ensuing decades to encompass more and more commercial, and even non-commercial, activity under its umbrella.[37] But the effects of this steady expansion of the definition of what constitutes a trade secret can only be comprehended when considered in tandem with the remedial power inherent in having a trade secret: the ability to keep that information private and protect it from any public dissemination, possibly forever. Should the trade secret leak out by misappropriation (i.e., theft, breach of confidence, and the like), the fundamental remedy for misappropriating a trade secret is an injunction against the misappropriator using the information for the life of the trade secret.[38] Such an injunction serves as a means to return what may have been briefly in the public's hands, or at least susceptible to public dissemination, back into private, and consequently secret, hands.[39] In

34. "The typical defendant in a trade secret case is a competitor who has misappropriated the plaintiff's business secret for profit in a business venture." DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 195 (Cal. Ct. App. 2004). It might be more accurately stated that such a typical defendant is one who has *allegedly* misappropriated a trade secret.

35. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

36. Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 248 (1998).

37. As discussed in more detail below, the definition of what constitutes a trade secret has expanded over time, as has the actual definition of a "secret" itself and possible relief when a trade secret is misappropriated. *See infra* Part III.B. Moreover, in many jurisdictions, governments and non-profit organizations can hold trade secrets. *See infra* Part IV.B.1.

38. *See* JAMES POOLEY, TRADE SECRETS § 7.02[2][a] (2005).

39. Interestingly and paradoxically, in at least one state, misappropriating a trade secret and disseminating it on the Internet is not sufficient to render the trade secret in the "public domain"

theory, if not always in practice, the trade secret injunction is the edifice that blocks the broader public from benefitting from the public (albeit unlawful) dissemination of the information.

Finally, it is worth noting one element of trade secrecy that benefits the public: Reverse engineering[40] and independent discovery are allowed. Such discovery is entirely lawful, and would allow the discoverer to use the trade secret in commerce.[41] Thus, if a user independently reveals the composition of a trade secret through his own efforts, that person is free to reap the rewards of the effort. However, because affirmative activity by those interested in learning the trade secret is required, a significant burden falls on the seeker of information to do the required work of discovery.

In order to understand how these elements of trade secrecy doctrine pose major problems when applied to public infrastructure, it is essential to first understand the theoretical construct of trade secret law and its development. By considering the values that drive trade secrecy, and its expansion in recent decades, the fundamental divergence with our traditional notions of accountable and open government become evident. Especially because the law's doctrinal development has been driven primarily by common law, the law's core underpinnings take a bit of a circuitous route through various jurisdictions, from courts to restatements, and only recently through legislatures.[42] Thus, a complete exploration

---

such that it is no longer considered a trade secret. *See* NEV. REV. STAT. ANN. § 600A.055 (West 2006).

40. Reverse engineering

> is the process of discovering the technological principles of a mechanical application through analysis of its structure, function and operation. It often involves taking something (e.g., a mechanical device, an electronic component, a software program) apart and analyzing its workings in detail, usually with the intention to construct a new device or program that does the same thing without actually copying anything from the original."

Wikipedia.org, Definition of Reverse Engineering, http://en.wikipedia.org/wiki/Reverse_engineering (last visited Oct. 16, 2006). Reverse engineering a trade secret is generally permissible. *See* CAL. CIV. CODE § 3426.1(a) (West 2006) ("Reverse engineering or independent derivation alone shall not be considered improper means.").

41. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) (noting that "discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering" is lawful and not precluded by trade secrecy law).

42. Indeed, one of the major differences between trade secrecy law and the other three major areas of intellectual property (trademarks, copyrights, and patents) is that those three areas have significant statutory support and history. *See* 15 U.S.C.A. §§ 1051-1072 (West 2006) (codifying trademark law); 17 U.S.C.A. §§ 101-122 (West 2006) (codifying copyright law); 35 U.S.C.A. §§ 100-105 (West 2006) (codifying patent law). Trade secrecy, on the other hand, has only recently been the subject of federal legislative consideration. *See* Economic Espionage Act (EEA) of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified as amended at 18 U.S.C.A. §§ 1831-1839 (West 2006)). Thus, in order to explore the underpinnings of trade secrecy, it is especially important to

requires consideration of these various sources of law.

A. *The Theoretical Framework of Trade Secrecy: Commerce*

From its inception as a doctrine, the basic theory of trade secrecy has maintained a singular focus on commercial activity. Among the many variables defining what constitutes a trade secret, commercial concerns have been the one bedrock constant throughout the law's development. The primary concerns of trade secret law are maintaining business ethics and the encouragement of the inventive spirit and innovation in businesses. Businesses rely upon trade secrecy to maintain competitive advantages, spur product development and innovation, and ultimately attempt to maximize capture of the economic benefits of their work.[43]

As discussed below, whether considered a function of property, tort, unfair competition, or contract, both commentators and courts historically have considered how trade secrecy law should be applied, and what results should be reached, by focusing on these commercial values and ideas.[44] Indeed, even when courts and legislatures have allowed trade secrets to be held by the government,[45] legislatures and courts have still relied upon commercial bases and rationales when defining their application and effect.[46]

---

review early case law and those opinions that became the classic statements of trade secrecy's definition, application, and purview.

43. *See* POOLEY, *supra* note 38, § 1.02[2]. The Supreme Court of Illinois adds a third policy consideration in favor of trade secrecy, also commercial in nature: the "public interest in having free competition in the sale and manufacture of goods not protected by a valid patent." Brunswick Corp. v. Outboard Marine Corp., 404 N.E.2d 205, 207 (Ill. 1980). At a general level of fair competition between commercial entities, there is nothing wrong with maintaining a secret for these reasons. If, on the other hand, secrecy is maintained in order to hide product deficiencies, limit public criticism, or deceive the public, then trade secrecy's underpinnings are mutated, and the justification for trade secrecy is undermined.

44. Whether trade secrets should be viewed as a right relating to property, tort, unfair competition, contract, or a combination thereof, and what this means for the development of the law, has been thoroughly analyzed, *see, e.g.*, Bone, *supra* note 36, at 245, but is not the focus of this Article. Moreover, it is not particularly relevant here, as the "dispute over the nature of trade secret rights has had little practical effect on the rules governing civil liability for the appropriation of a trade secret." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (1995).

45. This is a dangerous and, I believe, erroneous endeavor that will be discussed in some detail in Part IV.

46. *See, e.g.*, OHIO REV. CODE ANN. § 1333.61(C) (West 2006) (defining a person covered by Ohio's Uniform Trade Secrets Act as including government entities); Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1044 (2000) (arguing that the "government has the same right as private parties to classify information. If the material that it wishes to keep secret qualifies under the general trade secret laws, then like any private party it has the right to injunctive relief to prevent that information from slipping into hostile hands"). As I argue here, and explain more fully below, because the basic theoretical underpinnings of trade secrecy focus exclusively on commercial concerns, trade secrecy (as currently conceived) and government should not mix. The government

This theoretical conception of the world of trade secrets—as purely private matters between businesses or individuals—flows through the earliest caselaw and various restatements of the law, and drives the decisions of courts and legislators. Trade secret law, from its inception as a legal doctrine, envisaged commercial actors in competition for market share. Despite its recent application to the scenarios discussed here, the core elements defining a trade secret—maintained secrecy and connection to commercial activity—have not significantly changed in centuries.[47]

In one of the earliest United States court cases addressing trade secrets, a Massachusetts state court decision from 1837, a secret process for making chocolate was the trade secret at issue.[48] The plaintiff, a potential purchaser of a chocolate business, brought an action alleging that the terms of the sale included that the defendant-seller convey his secret formula to the plaintiff.[49] The defendant refused to convey it and argued that he had the right to retain the secret and share it with others.[50] In finding that the secret should have been conveyed with the business and holding that the requirement of conveying the secret was not a "restraint of trade," the Court summarized the purely private nature of the information and rights at issue:

> The defendant claims to operate by a *secret art*. The public are not prejudiced by the transfer of it to the plaintiff. If it were *worth any thing*, the defendant would use the art and keep it secret, and it is *of no consequence to the public* whether the secret art be used by the plaintiff or by the defendant.[51]

This case exhibits the fundamental elements of trade secrecy: the (1) "secret art," here, a business method of making chocolate, (2) focus on the secret's "value" to the business, and (3) the public's lack of general interest in which private party owns the secret.

In later opinions, courts continued to wrestle with whether allowing a secret business method was akin to a restraint of trade, but consistently

---

has more appropriate and doctrinally consistent avenues by which to "classify" information, like the various Freedom of Information Act (FOIA) exemptions that currently exist. *See infra* Part VI.

47. There is limited scholarship on the history of trade secrecy prior to the creation of the United States. *See, e.g.*, A. Arthur Schiller, *Trade Secrets and the Roman Law: The* Actio Servi Corrupti, 30 COLUM. L. REV. 837, 837-38 (1930) (discussing Roman application of trade secret principles). *But see* Alan Watson, *Trade Secrets and Roman Law: The Myth Exploded*, 11 TUL. EURO. CIV. L. R. 19 (1996) (challenging Schiller's conclusions). I focus here on trade secrecy's development in the United States, primarily because I seek to draw contrasts with certain governing values of American democracy.

48. Vickery v. Welch, 36 Mass. (1 Pick.) 523, 525 (1837).

49. *Id.* at 526.

50. *Id.*

51. *Id.* at 527 (emphasis added).

held that it was not because, among other reasons, the general public's interest in businesses' secrets was minimal.[52] In 1939, the American Law Institute published its seminal *Restatement (First) of Torts*.[53] This contained the first comprehensive effort in the United States to systematically define a trade secret and outline its parameters.[54] The authors posited that it was the maintenance of business competition ethics and proper means of acquiring knowledge, and not a property or similar right, that warranted liability for the misappropriation of a trade secret.[55] As they stated, "The theory that has prevailed is that the protection is afforded only by a general duty of good faith and that the liability rests upon breach of this duty; that is, breach of contract, abuse of confidence, or impropriety in the method of ascertaining the secret."[56] Again, purely private commercial interests were the focus.

Certainly after the *Restatement (First) of Torts*, if not sooner, there could be no doubt that trade secrecy was an exclusively commercial doctrine. Modern model codes and restatements echo this paradigm. The Uniform Trade Secrets Act, promulgated in 1979 and revised in 1985, cites *Kewanee Oil Co. v. Bicron Corp.* and notes that commercial ethics remain the focus of trade secret law.[57] Similarly, the contemporary *Restatement (Third) of Unfair Competition*, which inherited the doctrine of trade secrecy from the *Restatement (First) of Torts*,[58] notes several "interests" advanced by trade secrecy, all of which involve primarily commercial concerns: (1) "the unfairness inherent in obtaining a competitive advantage through a breach of confidence"; (2) encouraging investment by allowing trade secret holders to recapture the financial rewards of their innovations; (3) the "efficient exploitation of knowledge" by allowing for disclosure of information to "employees, agents, licensees, and others who can assist in its productive use"; and (4) "personal privacy."[59] Secrecy, backed by general standards of commercial ethics and norms, remained the constant. Indeed, the United States Supreme Court has recently reinforced this

52. *See* O. & W. Thum Co. v. Tloczynski, 72 N.W. 140, 144 (Mich. 1897) (hinging its willingness to maintain the secret of the business on the judgments that (a) secrecy was an acceptable business decision, (b) public interest allowed for the maintenance of an agreement to maintain a business secret, and (c) the public's right to the information was non-existent); Dr. Miles Med. Co. v. John D. Park & Sons Co., 220 U.S. 373, 402 (1911) (finding that a medicine manufacturer may rely "upon the ownership of its secret process and its rights are to be determined accordingly").

53. *See supra* note 1 and accompanying text.

54. POOLEY, *supra* note 36, § 2.02[1].

55. RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939).

56. *Id.*

57. UNIF. TRADE SECRETS ACT § 1 cmt., 14 U.L.A. 438 (1985); *see also supra* note 41.

58. This change apparently took place as the development of the law moved away from tort based theories to those of unfair competition. *See* RESTATEMENT (SECOND) OF TORTS 1-2 (1979).

59. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. a (1995).

conception, equating trade secrets with "domestic gossip or other information of purely private concern."[60]

As can be seen, from the earliest cases discussing the "secret art" of chocolate producers to the Supreme Court's modern day view of trade secrets as a "purely private" concern, courts, commentators, and authors of model codes and restatements have developed trade secrecy's parameters by conceptualizing the commercial actor in the business world competing with his rivals for commercially valuable information. That is a world where the public at large has no strong interest.[61] This, of course, makes intuitive sense when the goal is to maintain a level and fair playing field for all those who seek to operate or work for a profit-seeking business.

B. *Trade Secrecy Doctrine and Its Incongruous Elements*

The ever-expanding definition of a trade secret through a broadening of what constitutes "secrecy" and "commercial use," and how these doctrines have been applied (and misapplied) to more and more situations, amplifies the impact of trade secrecy in commerce. Additionally, the fact that a trade secret can be held forever makes the ability to hinder disclosure and public dissemination of information even more powerful. Inasmuch as trade secrecy is playing a major role in business operations and strategy, and businesses are increasingly entering the market for public infrastructure, the growing breadth of trade secrecy is a harbinger of increasing conflict as the worlds of private and public life mesh. To understand the magnitude of this expansion, the broad ambit of trade secrecy and its expansive application will be discussed briefly below.

1. What Is "Secrecy," and What Is Its Impact on the Public?

While secrecy is at the core of the trade secrecy doctrine,[62] the

60. Bartnicki v. Vopper, 532 U.S. 514, 533 (2001). *Bartnicki* has been the subject of much criticism because of its restrictive definition of a "public concern" that would justify speech notwithstanding the commercial interests and rights of trade secret holders. *See* Eugene Volokh, *Freedom of Speech and Intellectual Property: Some Thoughts After* Eldred, 44 Liquormart, *and* Bartnicki, 40 HOUS. L. REV. 697, 739-49 (2003) (commenting that the courts have a myopic view of what constitutes a "public concern," and, in any case, should not be the entity deciding what is a "public concern" for purposes of First Amendment analysis).

61. Based upon the above, now it should be no surprise that the Second Circuit Court of Appeals would state, "Although the bulk of trade secret law relates to industrial information, some kinds of non-industrial business information—for example, data related to customers, merchandising, cost and pricing, and systems and methods—are also protected." Lehman v. Dow Jones & Co., 783 F.2d 285, 298 (2d Cir. 1986) (citing 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 2.09[8] (1985)).

62. *Id.* at 298 (stating that "the most important consideration remains whether the information was secret").

Restatement (First) of Torts noted that the protection of trade secrets is "not based on a policy of rewarding or otherwise encouraging the development of secret processes or devices. The protection is merely against breach of faith and reprehensible means of learning another's secret."[63] Yet, the explanation in the Restatement begs the question: Isn't the encouragement of creating "secret processes or devices" precisely the byproduct and result of a law that values secrecy as its "most important consideration" in order for its protection to be operational? It would seem so, if the previously discussed empirical data derived from industry is to be believed.[64]

This answer is further underscored because "secrecy" results in lost opportunities to easily gain information and knowledge, a critical problem when the information involves the public infrastructure that all use.[65] The commercial benefits of secrecy accrue with no requirement of easy access to the information. This can be illustrated by briefly comparing patent and trade secrecy law. The basic patent trade-off—public disclosure of all elements of the patented work, be it a product, business method, or invention, in return for a limited-time monopoly granted to the patent owner—achieves the dual goals of public dissemination (transparency) and the ability to examine and confirm (if not necessarily profit from such knowledge, i.e., accountability) that are largely absent in trade secrecy. While one may not reproduce the patented work for profit, one may at least access the information relatively easily and attempt to build upon or critique it. But under trade secrecy law there is no opportunity for the general public to easily examine information deemed secret. As the Supreme Court noted in 1933, although monopoly rights are not granted with trade secrecy, there is no need for the trade secret holder to ever disclose the secret to the public.[66]

This difference has been discussed with reference to patents. One early commentator distinguished between using patentable information *in* public versus the use of information *by* the public, explaining:

> A use *in* public is not necessarily a use *by* the public. It is distinguished, not from an individual, but from a secret use.

63. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

64. *See supra* notes 10-12 and accompanying text. Of course, trade secret law keeps nothing secret per se; rather, it encourages and enables the protection of secrets and protects information that has lost its secrecy.

65. Easy access would be, for example, a simple request for the information or its general public availability by way of the Internet or another media device. No significant effort would be required, as compared to the potentially time-intensive work of reverse engineering, allowed under trade secrecy doctrine. Moreover, the fact that a trade secret that is reverse engineered may theoretically be used by those who make the effort does not change the fact that effort is required to access the information. *See supra* notes 40-41 and accompanying text.

66. U.S. v. Dubilier Condenser Corp., 289 U.S. 178, 185-86 (1933).

> It is *a use which places the invention in such a relation to the public that if they choose to be acquainted with it, they can do so.*[67]

Patent law allows the real possibility, and perhaps likelihood, of a use in public that offers easy opportunities for knowledge gained by the public. Trade secrecy, however, as applied to public infrastructure, is a use *in* public with little easy opportunity for knowledge gained *by* the public. It offers no such simple opportunity; its impact here is to deny the public the ability to "choose to be acquainted" with the relevant knowledge—to keep information secret.

Moreover, trade secrecy exacerbates the loss of public information because it encourages the strictest efforts to hide information from public view. The ease with which one may ascertain information generally determines whether the information may be deemed a secret. Thus, the right to trade secrecy protection is "defined by the extent to which the owner of the secret protects his interest from disclosure to others."[68] Indeed, the *Restatement (First) of Torts* listed six bases for determining whether information constitutes a trade secret, reflecting a clear focus on the owner's activities and a heavy burden placed on the owner of the secret to maintain secrecy:

> (1) the extent to which the information is known outside of [the] business; (2) the extent to which it is known by employees and others involved in [the] business; (3) the extent of measures taken by [the business] to guard the secrecy of the information; (4) the value of the information to [the business] and [its] competitors; (5) the amount of effort or money expended by [the business] in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others. . . .[69]

This places the onus squarely on the secret holder to prove that he has made efforts to keep the secret. In fact, only the sixth factor (the ability to reverse engineer) does not depend, at least in some part, on the efforts made to keep the secret.

But trade secrecy doctrine has taken an unusual course, and in doing so

67. Louis Burgess & Ralph Dinklage, *Secret Use in its Relation to the "Public Use" Provisions of R.S. 4886*, 28 J. PAT. & TRADEMARK OFF. SOC'Y 815, 818 (1946) (quoting 1 WILLIAM C. ROBINSON, THE LAW OF PATENTS FOR USEFUL INVENTIONS 434 (1890)).

68. DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 13 (Cal. 2003) (quoting Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984)).

69. Ashland Mgmt. Inc. v. Janien, 624 N.E.2d 1007, 1013 (N.Y. 1993) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)) (alteration in original).

has created alternate methods by which to establish a trade secret. The importance of that sixth factor is greater than one might expect, and its importance relative to other considerations increases the possibility of protecting information as a trade secret. Although this list of factors is still cited today,[70] its contours are often altered such that proving a secret can be achieved with less reference to the actual activities of the owner, or put another way, with less reference to the first five factors.[71] Referring to *Kewanee*'s definition[72] as an "early basic tenet of trade secrets law," one court recently explained, "Modern courts, however, have taken a different approach: 'Secrecy' may be measured by 'the ease with which information can be developed through proper means: if the information can be readily duplicated without involving considerable time, effort or expense, then it is not secret.'"[73] Surprisingly, the converse has also been found: "[I]nformation may be classified as a trade secret, regardless of its presence in the public domain or the ability of a competitor to acquire the information, based on the difficulty in discovering the trade secret, for example, through reverse-engineering."[74] The modern *Restatement (Third) of Unfair Competition* appears to support this alternate basis for establishing a trade secret.[75] Thus, the sixth factor seems to be more

70. *See* Australian Gold, Inc. v. Hatfield, 436 F.3d 1228, 1245 (10th Cir. 2006) (noting that Oklahoma utilizes these six factors).

71. *See* Amoco Prod. Co. v. Laird, 622 N.E.2d 912, 918 (Ind. 1993) ("'Although all of the Restatement's factors no longer are required to find a trade secret, those factors still provide helpful guidance to determine whether the information in a given case constitutes 'trade secrets' within the definition of the statute.'" (quoting Optic Graphics, Inc. v. Agee, 591 A.2d 578, 585 (Md. Ct. Spec. App. 1991))); *In re* Bass, 113 S.W.3d 735, 740 (Tex. 2003) ("We agree with the Restatement [(Third) of Unfair Competition § 39 cmt. d] and the majority of jurisdictions that the party claiming a trade secret should not be required to satisfy all six factors because trade secrets do not fit neatly into each factor every time.").

72. *See infra* note 94 and accompanying text.

73. Crane Helicopter Servs., Inc. v. United States, 56 Fed. Cl. 313, 323-24 (2003) (quoting C&F Packing Co. v. IBP, Inc., 224 F.3d 1296, 1302 (Fed. Cir. 2000)).

74. *Id.* at 324.

75. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (1995) ("[T]he requirement of secrecy is satisfied if it would be difficult or costly for others who could exploit the information to acquire it without resort to . . . wrongful conduct . . . ."). Of course, this might include considerations of how much a trade secret owner has actually attempted to guard the secret, but the spotlight on the inherent difficulty of reverse engineering moves the focus away from the owner's activities and more towards those of the alleged misappropriator. Alternatively, a trend towards devaluing reverse engineering as a defense to misappropriation, viewing it as a cover to obscure actual misappropriation, or both, is possible. Under the Economic Espionage Act (EEA) of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839 (West 2006)), which criminalizes some forms of trade secret theft, at least one commentator has noted that the status of reverse engineering as a defense to misappropriation is "ambiguous." *See* Craig L. Uhrich, *The Economic Espionage Act—Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. & TECH. L. REV. 147, 174 (2000-01).

important than the first five.[76] The result is that courts are increasingly tasked with the highly subjective job of determining what constitutes "difficult or costly" reverse engineering.[77]

In sum, the definition of a "secret" takes on unusual connotations under trade secrecy doctrine. One may develop a process that is extremely time-intensive and costly to reproduce, and do comparatively little to maintain its secrecy, and still call it a "secret." This is proper in the commercial world, as it rewards the time and effort expended in creating a valuable (or potentially valuable) service or process. However, as discussed in Part IV, to the public these many ways to secrecy create additional impediments to understanding the infrastructure upon which they rely. As explained by one California appellate court, the basic prohibition remains the same: "A trade secret is private property and belongs in the public domain if, and only if, the inventor sees fit to divulge it."[78] The effect of these unusual definitions is clear: More, and not less, information has the possibility of being protected by trade secrecy doctrine from unfettered public disclosure and examination.[79]

2. What is "Commercial Use"?

The definition of "commercial use" in trade secrecy doctrine has expanded greatly over the last seventy-five years, and its varying definitions have caused more information to fall under the protection of trade secrecy doctrine. The impact of this expansion is to create greater impediments to unfettered access to information. This extension can be seen by briefly tracing its contours in the Restatements and significant model codes and federal laws of the twentieth century.

From the days of the *Restatement (First) of Torts*,[80] the ensuing decades have seen an erosion of the requirement that the information actually be "continuous[ly] use[d] in the operation of a business." The Uniform Trade Secrets Act (UTSA), promulgated in 1979 and revised in 1985, affected a sea change in the contours of trade secrecy by requiring that the

76. *See Laird*, *supra* note 71, at 918 ("In determining whether information is protectable as a trade secret, '[t]he first and foremost consideration is whether the . . . information is readily accessible to a reasonably diligent competitor.'" (quoting Surgidev Corp. v. Eye Tech., Inc., 648 F. Supp. 661, 682 (D. Minn. 1986))).

77. *See* Flotec, Inc. v. S. Research, Inc., 16 F. Supp. 2d 992, 1001 (S.D. Ind. 1998) (stating that "[w]hether information is 'readily ascertainable by proper means' is a matter of degree . . . .").

78. Sinclair v. Aquarius Elecs., Inc., 116 Cal. Rptr., 654, 659 (Cal. Ct. App. 1974).

79. *See* Chiappetta, *supra* note 14, at 89 (noting that, in comparison to patents, "trade secret protection extends to an extremely wide variety of information"); Don Weisner & Anita Cava, *Stealing Trade Secrets Ethically*, 47 MD. L. REV. 1076, 1125 (1988) (commenting that the "legal definition of a trade secret is very undiscriminating and allows nearly all business ideas to qualify").

80. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) ("A trade secret is a process or device for continuous use in the operation of the business.").

"information, including a formula, pattern, compilation, program, device, method, technique, or process" derive "independent economic value, *actual or potential.*"[81] The comments to this section explained, "The broader definition in the proposed Act extends protection to a plaintiff who has not yet had an opportunity or acquired the means to put a trade secret to use."[82]

Thus, by 1985, the definition of a trade secret could include information that had not even been established in the business as commercially useful, as well as "business information."[83] In fact, utilizing similar definitions, courts have rejected arguments that information cannot be a trade secret where its value is merely a "hypothetical possibility."[84] Moreover, the definition includes negative data or information, such as "the results of lengthy and expensive research which proves that a certain process will *not* work."[85] In sum, the UTSA solidified the fact that an abundance of information, far beyond the purely "commercial," would be protected by trade secrecy. In the present context, this means that more public infrastructure information may be withheld from public inspection under trade secrecy law.

Evidencing how much lower the economic threshold for trade secrecy protection has fallen, 1995's *Restatement (Third) of Unfair Competition* explicitly states that the economic advantage afforded the trade secret owner "need not be great," and it would be "sufficient if the secret provides an advantage that is more than trivial."[86] Thus, virtually all information that may, in some more than trivial way, have any value to a company could qualify as a trade secret. The federal Economic Espionage Act (EEA) of 1996, which criminalizes most forms of misappropriation, is perhaps the ultimate culmination of the elimination of the "continuous use" requirement in trade secrecy law. It builds upon the UTSA definition, and includes virtually all business information, including business plans and customer lists.[87]

By 2005, a form of the UTSA had been adopted in forty-four states and

81. UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 438 (1985) (emphasis added).

82. *Id.* § 1 cmt.

83. *See* Carbo Ceramics, Inc. v. Keefe, 166 Fed. App'x 714, 720 (5th Cir. 2006) (holding that "there was abundant evidence for a reasonable jury to conclude that [plaintiff] had a trade secret in its business plans and strategies, including pricing for its products as well as detailed information regarding industry trends, customers, and customer preferences").

84. *See* Joint Stock Soc'y v. UDV N. Am., Inc., 104 F. Supp. 2d 390, 409 (D. Del. 2000) (involving the question of whether sealed recipes to make "flavored vodkas and liqueurs" should be unsealed, and upholding the special master's application of trade secrecy protection to the plaintiff's vodka recipes under the Delaware Trade Secrets Act, in part because while "these vodka recipes may be old, they are nevertheless a source of potential value to the defendants").

85. UNIF. TRADE SECRETS ACT § 1 cmt.

86. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. e (1995).

87. 18 U.S.C.A. § 1839(3) (West 2006); POOLEY, *supra* note 38, § 13.03[2].

the District of Columbia.[88] The *Restatement's* "continuous use" requirement is largely dead.[89] Untethering the "commercial use" factor from actual "economic value" has substantially expanded the potential application of the trade secrecy doctrine to virtually any form of information connected to a business.[90] The public suffers from an increasing inability to access information, which in the context of, for example, whether a voting machine is properly tabulating votes, is troublesome. Regardless of this concern, the current trend is towards more, rather than less, business information being subject to trade secret protection. The myriad complications that this creates are discussed in Part V.

3. The Infinite Possible Duration of a Trade Secret

Aside from the broad definition of "secret" and the limited need for information to have commercial currency, one consistent element in trade secrecy doctrine is the theoretical unlimited duration of a trade secret. So long as the elements of trade secrecy are met, the right to keep a secret for an infinite period of time underscores the real power of enjoying trade secret protection. For instance, the "secret combination of flavoring oils and ingredients known as 'Merchandise 7X,'" the formula for Coca-Cola, which is not patented, is the most famous example of a trade secret and has existed as a trade secret for over 100 years.[91] Why would Coca-Cola choose trade secrecy over patents? Precisely because of the infinite duration of trade secret protection; Coca-Cola bet on its ability to maintain the secret, and by doing so afforded itself protection (and the concomitant pecuniary gain attendant to a monopoly) far beyond the twenty-year limit of patent protection.[92]

---

88. POOLEY, *supra* note 38, § 2.03[7][a]. It should be noted that the states have made alterations to the UTSA on a state-by-state basis, but, as one commentator has noted, the similarities in substance between the states are greater than differences in the language used. *Id.* § 2.03[7][c].

89. *See* Bone, *supra* note 36, at 249-50 (noting that the continuous use requirement has been "relaxed or ignored" in recent years).

90. *See id.* at 248 (noting that "almost anything can qualify as a trade secret, provided it has the potential to generate commercial value"). However, it is possible that even this statement is too narrow, as commercial value is now required at something just above trivial.

91. *See* Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D. 288, 289 (D. Del. 1985). Noting the efforts that Coca-Cola has undertaken to protect its secret, the court explained that the formula "has been tightly guarded since Coca-Cola was first invented and is known by only two persons within The Coca-Cola Company" and that the "only written record of the secret formula is kept in a security vault at the Trust Company Bank in Atlanta, Georgia, which can only be opened upon a resolution from the Company's Board of Directors." *Id.*

92. Daniel N. Christus et al., *Intellectual Property in the Americas*, 13 AM. U. INT'L L. REV. 1095, 1099 (1998) ("The decision of whether or not to patent the Coca-Cola formula came down to a question of whether they wanted to have a seventeen year monopoly or whether they wanted

State statutes also prescribe that a "trade secret endures and is protectable and enforceable until it is disclosed or discovered by proper means."[93] Because a trade secret lasts, at least in theory, as long as a trade secret holder maintains its secrecy, the possibility that the information will never enter the public domain is very real. Whatever benefits the public might gain from unfettered access to the information is lost, so long as secrecy is maintained, the possibility of independent discovery of the trade secret is low, and active efforts like reverse engineering are unsuccessful. Thus, the choice of trade secrecy offers the benefit of a monopoly on the information for a potentially infinite period of time.

In sum, trade secrecy, as currently configured, is a pervasive and powerful tool for business. Its contours and scope of protection are expanding along with its power as a device to maintain privacy and secrecy. Although one may quibble at the margins regarding the likelihood of independent discovery of a trade secret, whether a trade secret may really be kept forever, or whether trade secrecy is chosen over patent in every sector important to public infrastructure, there is little dispute that trade secrecy remains a dominant intellectual property strategy for many businesses. We now turn to examine how the values that animate trade secret law align with those animating the provision of public infrastructure.

IV. THE VALUES AND PRIORITIES OF OPEN GOVERNMENT

The conflict between trade secrecy and a transparent and accountable democratic government is ultimately a clash of governing theory and values. Trade secrets, by their very name, have secrecy as the default position; while loss of protection and consequential transparency can and does happen, recognition of the value of secrecy remains its governing principle.[94] In contrast, democratic government operates by diametrically opposed values, which I define for these purposes and explain below as transparency and accountability. While there are exceptions, especially after the passage of the Freedom of Information Act (FOIA), democratic government is driven by notions of transparency and accountability.[95] Secrecy is the exception, rather than the norm. When considering these contrasting goals and values, it becomes apparent that trade secrecy and

to rely on the [sic] their ability to keep this a trade secret forever.") (comments by Robert Wagner). Again, unlike trade secrecy, a patent affords the public the ability to examine the information, and after the twenty-year term of the patent, to use that information in commerce. Thus, the public can design around the information to create new processes that can expand our knowledge base.

93. S.C. CODE ANN. § 39-8-30 (2005).

94. As explained by the Supreme Court, trade secret material "must be secret, and must not be of public knowledge or of a general knowledge in the trade or business." Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974).

95. *See* 5 U.S.C.A. § 552 (West 2006).

public accountability cannot easily coexist.

A. *The Public Values of Transparency and Accountability*

In order to grasp the fundamental conflict between trade secrecy applied by private providers of public infrastructure and the democratic values of transparency and accountability, it is important to briefly examine how these two values orient government as we know it today.[96] The prominence of the values of transparency and accountability in our assumptions about how government should work makes the overlay of trade secrecy problematic. The contours of their practical application in society highlight the disconnect between accountability and trade secrecy, but also suggest some of the remedies to the problem.

In the mid-nineteenth century, Jeremy Bentham eloquently developed the values and benefits inherent in a government that is open to public inspection. While noting that maintaining secrets may have some short-term benefits, Bentham succinctly stated that in "an assembly elected by the people, and renewed from time to time, publicity is absolutely necessary to enable the electors to act from knowledge."[97] He explained:

> To conceal from the public the conduct of its representatives, is to add inconsistency to prevarication: it is to tell the constituents, "You are to elect or reject such or such of your deputies without knowing why—you are forbidden the use of reason—you are to be guided in the exercise of your greatest

96. It is important to note that I am not suggesting that government always, or even often, operates in this manner, but that it should and that these values are imbued into our government. Nor is this Article intended as a survey of democratic values and institutions generally. Clearly, government often operates in the shadows and against the values of transparency and accountability. *See generally* PHILIP H. MELANSON, SECRECY WARS: NATIONAL SECURITY, PRIVACY, AND THE PUBLIC'S RIGHT TO KNOW (2001) (analyzing and detailing various efforts of the United States government to keep information secret, even where there is no basis to do so). While events like the recent scandal involving lobbyist Jack Abramoff and his illegal campaign contributions to various members of Congress underscore the fact that our government often does business in relative secrecy, it is telling that Senate Majority Leader Bill Frist's reaction to the revelation of the scandal was to state that he intends to "examine and act on any necessary changes to improve transparency and accountability for our body when it comes to lobbying." *See* Elana Schor, *Lieberman Signs on to McCain Lobbying Reform Bill*, THE HILL, Sept. 26, 2006, *available at* http://www.hillnews.com/thehill/export/TheHill/News/Frontage/010406/web.html. Faced with this scandal, Frist cited "transparency and accountability" as the answer. *Id.* For purposes of this Article, whether this will actually happen is less important than the fact that he cited those values as the proper governmental solution to the scandal of illegal lobbying contributions that allegedly took the form of bribes. *See id.*

97. JEREMY BENTHAM, *An Essay on Political Tactics* (1791), *reprinted in* 2 THE WORKS OF JEREMY BENTHAM, 299, 310-12 (John Bowring ed., Russell & Russell 1962) (1837); *see also* SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 171, 174-75 (1982) (discussing Bentham's contributions to this area).

powers only by hazard or caprice."[98]

Significantly, Bentham did not merely suggest openness as a rallying cry for the sake of the public, but openness as a benefit to the government as well. Although somewhat antiquated and perhaps naïve, his was a call to arms that government should maintain as open a policy as possible:

> But in an open and free policy, what confidence and security—I do not say for the people, but for the governors themselves! Let it be impossible that any thing should be done which is unknown to the nation—prove to it that you neither intend to deceive nor to surprise—you take away all the weapons of discontent. The public will repay with usury the confidence you repose in it. Calumny will lose its force; it collects its venom in the caverns of obscurity, but it is destroyed by the light of day.[99]

Not merely advocating a utilitarian reason for openness, Bentham argued that government operates both more efficiently and, more importantly, legitimately when the rights of the people to know what their government is doing—the "open and free policy"—are respected. Thus, the core benefit became accountability to the electing public through transparency: "The best project prepared in darkness, would excite more alarm than the worst, undertaken under the auspices of publicity."[100]

Perhaps the best modern-day statement of these core values is found in the passage of FOIA.[101] FOIA, enacted in 1966 as a result of increased interest in allowing investigative journalism,[102] is designed to force disclosure and "permit access to official information long shielded unnecessarily from public view"[103] by permitting any citizen (and indeed, businesses) to request information from the government by way of a FOIA request.[104] As explained in the introduction to one of the core studies of the rights of citizens to government information, "Few aspects of government-citizen relations are more central to the responsible operation of a representative democracy than the citizen's ability to monitor

98. *See* BENTHAM, *supra* note 97, at 312.

99. *Id.* at 310-11.

100. *Id.* at 310.

101. Of course, the need for FOIA in the first place suggests that there are barriers to transparency in government. Were it the general practice of government to share information that is not subject to serious misuse, then perhaps FOIA would be unnecessary. Transparency needed to be forced, but the fact that it was speaks volumes about the priority placed on this value.

102. Christopher J. Lewis, *When Is A Trade Secret Not So Secret? The Deficiencies of 40 C.F.R. Part 2, Subpart B*, 30 ENVTL. L. 143, 153 (2000).

103. EPA v. Mink, 410 U.S. 73, 80 (1973); *see also* Dep't of the Air Force v. Rose, 425 U.S. 352, 361 (1976).

104. Lewis, *supra* note 102, at 153.

governmental operations. Critical in this regard is the existence of a general individual right of access to government-held information."[105]

Notwithstanding this goal, FOIA recognizes that some information should be secret. Therefore, FOIA includes a number of exemptions from disclosure, including those for certain documents and information regarding national defense,[106] foreign policy,[107] law enforcement,[108] and, as determined by the federal agency holding the information, commercial trade secrets.[109] As explained by the Supreme Court, Congress felt the need for a trade secret exemption because "with the expanding sphere of governmental regulation and enterprise, much of the information within [g]overnment files has been submitted by private entities seeking [g]overnment contracts or responding to unconditional reporting obligations imposed by law."[110] Despite the protection of trade secrets, FOIA sets a default of disclosure[111] unless one of the exemptions applies. This default position effectively orients government towards disclosure and away from secrecy (the opposite of trade secrecy, which protects secrecy except in limited circumstances).[112]

Undeniably, government openness is recognized in a variety of modern laws and rules. There are a number of examples of the value that the United States government places on transparency.[113] They include judicial decisions and statutes,[114] the exemption from copyright protection for

105. Project, *Government Information and the Rights of Citizens*, 73 MICH. L. REV. 971, 971 (1975).

106. *See* 5 U.S.C.A. § 552(b)(1) (West 2006).

107. *See id.*

108. *See id.* § 552(b)(7).

109. *See id.* § 552(b)(4).

110. Chrysler Corp. v. Brown, 441 U.S. 281, 292 (1979).

111. The very existence of a trade secret definition designed specifically for FOIA suggests that the commercial definition is inappropriately applied to entities that operate in the governmental or public infrastructure spheres. *See generally* FOIA Update, FOIA Counselor, U.S. Dep't of Justice Webpage, http://www.usdoj.gov/oip/foia_updates/Vol_IV_4/page6.htm (last visited Oct. 15, 2006) (questioning a broad application of trade secret law in light of then recent case law).

112. Additionally suggesting the orientation of democratic government towards openness is what, in Australia, is known as the "reverse onus principle" for government secrets: "In order for the court to be persuaded to protect a government secret, the government must establish that it is in the public interest that the information not be disclosed. Further, the courts have been sceptical [sic] of governments wishing to keep matters secret so that the onus on the government is a heavy one." Pat Barrett, Public Private Partnerships—Are There Gaps in Public Sector Accountability?, 2002 Australasian Council of Public Accounts Committees (Feb. 3, 2003) (quoting AUSTRALIAN SENATE FIN. & PUB. ADMIN. REFERENCES COMM. COMMONWEALTH CONTRACTS: A NEW FRAMEWORK FOR ACCOUNTABILITY (2001), http://www.anao.gov.au/WebSite.nsf/Publications/CF07591C2441E5E74A256CC5002309BF.

113. Sandeen, *supra* note 4, at 398-400 (explaining the bases for government openness and considering various exceptions to secrecy and control of information in government).

114. *Id.* (citing H.R. REP. NO. 94-1476, at 58-59 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5671-73).

works of authorship created by United States government employees,[115] and the fact that governments post information on government websites.[116] One court's explanation of the grounds for the government's exemption from copyright protection is that the prohibition is "based on 'the necessity of wide public dissemination of the contents of materials produced by and relating to issues and problems of national interest . . . [which] policy is unquestionably a desirable one in a democracy, much of whose success is dependent on a well informed public.'"[117] The well-informed public, a basic value, is served by the absence of secrecy in information deemed "of national interest" and therefore without a right to be obscured.

This value is now received wisdom in government, even in a society increasingly transfixed with security issues. For example, Newt Gingrich, former Speaker of the House of Representatives, promised that all congressional documents and all House of Representatives conference and committee reports would be filed electronically so that they would be "available to any citizen in the country at the same moment it is available to the highest-paid Washington lobbyist."[118] Similarly, Federal Reserve Chairman Ben S. Bernanke's Senate testimony in November 2005 stated that he supports monetary policy that is "increasingly transparent to the public" because, among other reasons, a "more transparent policy process increases democratic accountability."[119] These comments make one thing clear: These values are entrenched in democratic government operations. Government policies are thus often analyzed or criticized based upon their adherence to these principles.

Of course, current government operations show that while politicians may profess support of these values, in many instances these values may not actually be followed. Consider the terrorist attacks on September 11, 2001, the single most significant event causing the recent major reversal of government openness. After the attacks, Attorney General John Ashcroft revised FOIA standards to decrease the amount of information subject to disclosure.[120] Although secrecy is sometimes justified, resulting

115. *See id.* (citing 17 U.S.C.A. § 105 (West 2006)).

116. *Id.*

117. Scherr v. Universal Match Corp., 297 F. Supp. 107, 110 (S.D.N.Y. 1967) (quoting 12 ASCAP COPYRIGHT LAW SYMPOSIUM 96, 105 (1961)); *see supra* note 114 and accompanying text.

118. James Love & Tim Hubbard, *Paying for Public Goods*, *in* CODE: COLLABORATIVE OWNERSHIP AND THE DIGITAL ECONOMY 207, 208 (Rishab Aiyer Ghosh ed., 2005) (quoting CONTRACT WITH AMERICA: THE BOLD PLAN BY REP. NEWT GINGRICH, REP. DICK ARMEY AND THE HOUSE REPUBLICANS TO CHANGE THE NATION (Ed Gillespie et al. ed., 1994)).

119. *Nomination of Ben S. Bernanke: Hearing on Nomination of Ben S. Bernanke to Become Chairman of the Federal Reserve System Before the S. Comm. on Banking, Housing, & Urban Affairs*, 109th Cong. 15 (2005) (testimony of Ben S. Bernanke).

120. *See* Press Release, U.S. Dep't of Justice, New Attorney General FOIA Memorandum Issued (Oct. 15, 2001), *available at* http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm. Interestingly, the United States General Accounting Office found that 31% of federal agencies

in the spotty and haphazard application of democratic values, the concepts of transparency and openness still influence the system of government that the United States regards as most legitimate and stable. A far cry from Bentham's ideal, they remain values worth considering, and emulating, when analyzing the effects of trade secrets in our public infrastructure.

B. *Conflict from a Theoretical and Practical Perspective*

The application of a doctrine designed to protect the competitive rights of a chocolate producer[121] runs into problems when the product is not chocolate, but voting machines. Once there is a deviation from purely commercial concerns towards other goals for which trade secrecy was not designed, like the quasi-governmental activity of providing public infrastructure, the disconnect becomes severe. Trade secrecy and democratic values collide in the private provision of public infrastructure. As discussed more thoroughly below, trade secret law has a profound but varying effect on both the ability of the public to easily access information about public infrastructure, and on the government's capability to access information that it deems necessary to serve and protect the public's interest. The law effectively keeps secret the very operations of our infrastructure and gives such protection the imprimatur of good policy.

Moreover, trade secrecy is now being directly linked to national security issues. Thus, as the Federal Bureau of Investigation launches a new effort to help United States businesses protect their trade secrets from foreign thieves,[122] and the Association of Corporate Counsel lobbies Congress to amend the USA PATRIOT Act to further protect business trade secrets from the Act's broad investigative powers,[123] some consideration must be given to the countervailing concern that too much protection may violate the public's right to information about their essential public infrastructure, especially when provided by commercial entities. As *The Oregonian* recently editorialized regarding the efforts of two of Portland's investor-owned energy utilities to keep their dealings with failed energy giant Enron secret,

> The most basic protection that consumers and investors have against fraud is information. Enron and its fellow conspirators literally lurked in the shadows—even the

---

decreased their release of information since this memorandum was released, a surprisingly low number. *See* U. S. GEN. ACCOUNTING OFFICE, FREEDOM OF INFORMATION ACT: AGENCY VIEWS ON CHANGES RESULTING FROM NEW ADMINISTRATION POLICY 14, 24 (2003), *available at* http://www.gao.gov/new.items/d03981.pdf.

121. *See* Vickery v. Welch, 36 Mass. (1 Pick.) 523, 523-24 (1837).

122. Kent Hoover, *FBI to Help U.S. Businesses Protect Secrets*, BIZJOURNALS, Jan. 23, 2006, http://www.bizjournals.com/extraedge/washingtonbureau/archive/2006/01/23/bureau1.html.

123. Robert Block, *Bush Antiterror Plans Irk Big Business*, WALL ST. J., Nov. 28, 2005, at A4.

> blackouts, in Enron's case—where light could not be shed on their dealings.
>
> The best way to avoid a repetition of such schemes is to make sure that public policy in Oregon continues to provide the citizens of the state with open information on the operation of the electric infrastructure that is critical for their lives.[124]

This example, and others described below, poses the ultimate question: Should we allow private firms providing public infrastructure—even when provided without significant government funding[125]—to enjoy that same level of trade secrecy protection? The answer must be no. After examining the interaction of these divergent theories and considering their application in practice, what becomes clear is that, for example, FOIA's specifically tailored exemptions from public disclosure—considered in the context of a default position of transparency—are far more suited to private entities engaged in the provision of public infrastructure than the broad doctrine of trade secrecy. More broadly, it becomes clear that trade secrecy creates far more problems than it solves when applied to public infrastructure.

1. The Current General Position of Courts and Commentators

In 1983, the Pennsylvania Commonwealth Court held what might seem intuitive to some: A "trade secret contention ceases to be of any moment when the function is recognized as governmental, rather than that of a private business."[126] This opinion, however, is a minority view. Despite these seemingly divergent goals and responsibilities, governments are often allowed to hold their own information as trade secrets.[127] And indeed, commentators as renowned as Professor Epstein have taken the position that "government has the same *right* as private parties to classify information."[128] Epstein argues that so long as government meets the relevant standard to establish a trade secret, it should be able to avail itself of that protection and seek "injunctive relief to prevent that information from slipping into hostile hands."[129]

---

124. Robert McCullough, Op-Ed., *Utilities and Trade Secrets*, THE OREGONIAN, Feb. 15, 2006, at C09, *available at* http://www.oregonlive.com/commentary/oregonian/index.ssf?/base/editorial/1139957734174280.xml&coll=7.

125. Many businesses receive some form of public funding, whether by grants, subsidies, or tax breaks. Here, I distinguish between government funded research and development, where keeping such secrets from government is difficult to justify, and purely privately funded and developed public infrastructure. It is this latter and more doctrinally challenging category that I consider here.

126. Hoffman v. Pennsylvania, 455 A.2d 731, 733 (Pa. Commw. Ct. 1983).

127. Epstein, *supra* note 46, at 1044.

128. *Id.*

129. *Id.* (emphasis added).

Professor Epstein's position is hardly controversial. As noted earlier, the *Restatement (Third) of Unfair Competition* mentions without explanation that governmental organizations, among others, can hold trade secrets, although the examples of trade secrets that it cites are more geared towards non-profit and charitable organizations.[130] Additionally, the UTSA's definition of "persons" subject to trade secret protection includes governments and governmental subdivisions and agencies, again without any analysis or commentary.[131] Thus, commentators, legislators and courts have been willing to extend trade secret protection to governmental and non-profit entities.[132]

2. Underlying Problems with Applying Trade Secret Law to Public Infrastructure

To argue that government has a "right" to trade secrets seemingly ignores the fundamental difference between a purely commercial entity distributing private commercial goods and services, and an entity operating in the public infrastructure sphere. Government commercial activity is notably absent from both our traditional view of government and core democratic values, and it is in that absence that the conflict between trade secrecy and democratic values resides. At the elementary level, government should not be in the business of keeping information secret just because it might have pecuniary value.

Trade secret law cannot be easily squared with the notion that commercial value is not a relevant consideration, at least not without changing the very purpose of the law. Creating law that allows a business to ethically maintain and increase its commercial power is its laudable policy and purpose. What trade secret law does not contemplate is a private actor taking on the role, if not the actual full responsibility, of a

130. RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 39 cmt. d (noting that "lists of prospective members or donors" are examples of "economically valuable information" that a governmental entity might claim as a trade secret).

131. UNIF. TRADE SECRETS ACT § 1(3), 14 U.L.A. 438 (1985).

132. Although not a focus of this Article, it is worth noting that a line of California federal cases have held that a non-profit organization, in these cases the Church of Scientology, could hold trade secrets if it met California's statutory requirements. *See* Bridge Publ'ns, Inc. v. Vien, 827 F. Supp. 629, 633-34 (S.D. Cal. 1993) (holding that the Church's "Advanced Technology" spiritual materials met the California statutory definition of a trade secret because, among other reasons, the Church "use[d] proceeds from the sale of these materials . . . to support the operations" of the Church); Religious Tech. Ctr. v. Scott, 869 F.2d 1306, 1308 (9th Cir. 1989) (noting that the court had previously held that the Church's "scriptures" were not trade secrets because the Church had not alleged any commercial value assigned to them); Religious Tech. Ctr. v. Netcom On-Line Commc'n. Servs., Inc., No. C-95-20091 RMW, 1997 U.S. Dist. LEXIS 23572, at *42 n.17 (N.D. Cal. Jan. 6, 1997) (entering a preliminary injunction against the disclosure of certain Church trade secrets and noting that it is difficult to identify "potential competitors" of the Church for purposes of the public knowledge element of the definition of a trade secret).

public-oriented institution like government. The vastly divergent roles and responsibilities of government, like transparency and accountability, versus industry's premium on secrecy, profit-making, and competition, make the application of trade secrecy to public institutions—or private entities operating in the public sphere—troubling.[133]

As a general matter, economist Joseph Stiglitz and others assert that "a governmental entity should generally not be allowed to withhold information from the public solely because it believes such withholding increases its net revenue."[134] Similarly, in the analogous case of government contracting for services, Professor Minow has advocated that such contracting "should not exempt the resulting activities from adherence to public values."[135] In that context, Hungary's "national ombudsman" has stated that regarding the relationship between public funds and private business, "[t]he transparency and controllability of the privatization processes, as public interest, takes precedence over the private interest of protection of business secrets."[136] Building on these assertions, I argue that a private entity engaged in the governmental activity of providing public infrastructure should be held to a high standard of accountability to the public. If we choose to maintain trade secrecy in its current form, we run the risk of turning our infrastructure, upon which the public relies to conduct its day-to-day activities, into just another product that is bought and sold.

This outlook change should happen because of the fundamentally

133. Barrett, in his sweeping analysis of Australia's infrastructural public-private partnership (PPP) arrangement, succinctly lays out the differing roles of commercial and public entities:

> Unlike purely commercial entities, public service providers are required to simultaneously account for (among other things) client satisfaction, the public interest, fair play, honesty, justice, security and equity as well as striving to maximise 'value for money'. The additional requirements derive, ultimately, from the 'political' judgement passed (at intervals, through the electoral process) on democratically elected governments' stewardship of public resources. The range and relative importance of these additional requirements vary at points in time and over time, not least because of changing public perceptions and expectations. However, they remain the distinguishing feature of public sector accountability compared to demands made of the private sector.

Barrett, *supra* note 112 (spelling in original).

134. JOSEPH STIGLITZ ET AL., THE ROLE OF GOVERNMENT IN A DIGITAL AGE 70 (2000), *available at* http://archive.epinet.org/real_media/010111/materials/stiglitz.pdf. Interestingly, Stiglitz conversely argues that public entities should be entitled to hold patents "if only to avoid allowing the patent to be reserved by someone else." *Id.*

135. MARTHA MINOW, PARTNERS, NOT RIVALS 142 (2002).

136. Kenneth K. Baar, *Open Competition, Transparency, and Impartiality in Local Government Contracting Out of Public Services*, *in* NAVIGATION TO THE MARKET: REGULATION AND COMPETITION IN LOCAL UTILITIES IN CENTRAL AND EASTERN EUROPE 112 (Tamás M. Horráth & Gábor Péteri eds., 2001), *available at* http://lgi.osi.hu/publications/2001/76/Reg-Ch2.PDF.

opposed value structures of government and commerce. This distinction is starkly evident when considering the historical values driving people to pursue public-oriented endeavors. While it may seem quaint today, it was not terribly long ago that the Supreme Court noted, in the context of considering whether government employees should be awarded patents for work performed while employed by the government: "It has been said that many scientists in the employ of the government regard the acceptance of patent rights leading to commercial rewards in any case as an abasement of their work."[137] In testimony before the Senate Committee on Patents, an employee of the Federal Bureau of Standards explained:

> [A] good many scientific men object to applying for a patent because they feel that it looks as though they were working primarily for profit when in fact they are not; when they are working for the development of science or perfecting some particular process or method to which they have been appointed.[138]

Of course, it is absurd to think that accepting a patent would be an "abasement" of the work of a privately employed scientist; quite the opposite, this achievement would be viewed as part of the scientist's job, and personal pride and financial compensation would likely be its reward. Moreover, the profit motive is the ultimate charge of a business, and a business' employees, including those who may develop patentable inventions and processes, share that common goal.[139]

Conversely, those employed by government are not charged with the institutional goal of turning a profit.[140] Intuitively, this must, in some measure, change the perspective that individuals bring into their employment, and that perspective should drive the orientation of the institution. To suggest to a government scientist that she should orient her efforts towards maximizing income to the government is almost as absurd as telling a privately employed scientist that she should uniformly and always consider the interests of the public over the interests of her employer to turn a profit and remain in business.[141] Both changes in orientation would require the employee to diminish in her mind and

137. United States v. Dubilier Condenser Corp., 289 U.S. 178, 219 (1933) (citing *Exploitation of Inventions by Government Employees: Hearing on S. 5065, S. 5066, and S. 5265 Before the S. Comm. on Patents*, 65th Cong. 16-17 (1919) (statement of James T. Newton, Commissioner of Patents)).

138. *Exploitation of Inventions by Government Employees: Hearing on S. 5065, S. 5066, and S. 5265 Before the S. Comm. on Patents*, 65th Cong. 17-18 (statement of E.B. Rosa, Chief Assistant, Bureau of Standards).

139. STIGLITZ ET AL., *supra* note 134, at 69.

140. *Id.*

141. *Id.* at 72-74.

actions the main purpose for the existence of her employer. Thus, the differing value structures found in the private and public sectors undermine the application of an expansive commercial trade secrecy doctrine to public infrastructure.

Moreover, the clash is evident when considering the fundamental difference between the reasons that a government might wish to keep information secret, like to protect the security of the nation, and a business's trade-based and profit-oriented reasons.[142] Because of these differences, courts have occasionally, and in my view, properly, refused to apply trade secret law in the public sphere. For example, as held by the Ohio Supreme Court considering this very question:

> Respondents cite no authority, however, holding that a public office can even *have* its own protected trade secrets . . . [T]his court has held that the fact that disclosure of information will result in a competitive disadvantage to the public institution is not grounds for preventing disclosure . . . The protection of competitive advantage in private, not public, business underpins trade secret law.[143]

Although subsequently superseded by a UTSA-based statute that now allows governments to hold trade secrets,[144] as the Ohio Supreme Court decision explained, governments simply do not engage the same goals or motivations as private sector entities.[145] Despite the regrettable fact that Ohio discarded this distinction, it is a distinction with profound meaning.

In fact, the United States Supreme Court has also recognized this difference.[146] It permitted the government to take aerial photographs of the industrial complex of a regulated company, and denied that company trade secret protection against those acts, utilizing, in part, similar logic: "Whether they may be employed by competitors to penetrate trade secrets is not a question presented in this case. Governments do not generally seek to appropriate trade secrets of the private sector, and the right to be free of

142. *Id.* at 69.

143. State *ex rel.* Toledo Blade Co. v. Univ. of Toledo Found., 602 N.E.2d 1159, 1163-64 (Ohio 1992) (citations omitted), *superseded by statute*, OHIO REV. CODE ANN. § 149.43(A)(1)(p) (West 2000), *as recognized in* State *ex rel.* Besser v. Ohio State Univ., 721 N.E.2d 1044, 1051 (Ohio 2000) (noting that Ohio UTSA now allows for governments to have trade secrets).

144. *Besser*, 721 N.E.2d at 1051. This statutory change does not automatically mean that the government can maintain a trade secret. *See* State *ex rel.* Dayton Newspapers v. Dayton Bd. of Educ., 747 N.E.2d 255, 259 (Ohio Ct. App. 2000) (applying the Ohio UTSA and *Besser* standard but finding no basis for trade secret protection of the names, applications, and resumes of people who applied for a position with the Dayton Board of Education, and explaining that the court failed to see "what independent economic value the . . . information has or how other private persons could reap some economic benefit from having it").

145. *Besser*, 721 N.E.2d at 1049.

146. *Dow Chem. Co. v. United States*, 476 U.S. 227, 231-32 (1986).

appropriation of trade secrets is protected by law."[147] Again, the Court acknowledged the distinction between public and private actors and their respective roles in regulating and conducting commerce, and found that commercial trade secret law was not applicable.[148] More significantly, the Court distinguished the application of trade secret law in this context by focusing on the law's very reasons to exist, and found the absence of those policy imperatives grounds to deny its application.[149] As these opinions show, analysis of trade secret protection when the actor's goals are not profit-oriented can render the entire doctrine inapplicable, if not entirely irrelevant.

Further illustrating this incongruity is the fact that courts have also recognized that even when applying trade secret law to governmental activity, utilizing a broad commercial definition of a trade secret is not appropriate when the focus is public values such as disclosure of information through transparency. For example, in rejecting the use of the Restatement of Torts definition of a trade secret[150] in FOIA's commercial trade secrets exception to disclosure,[151] the United States Court of Appeals for the District of Columbia Circuit explained:

> [T]he [Restatement of Torts] definition, tailored as it is to protecting businesses from breaches of contract and confidence by departing employees and others under fiduciary obligations is ill-suited for the public law context in which FOIA determinations must be made. . . . The common law definition was tailored to private contexts where public policy almost exclusively focuses on the unjust enrichment and competitive harm resulting when someone acquires a business intangible through the breach of a contract or a confidential relationship. . . . The Restatement approach, with its emphasis on culpability and misappropriation, is ill-equipped to strike an appropriate balance between the competing interests of regulated industries and the general public.[152]

Thus, the court chose a narrower definition that allowed the disclosure of "health and safety data" regarding intraocular lenses submitted by regulated companies to the United States Food and Drug Administration (FDA), despite the trade secrets exemption to FOIA.[153] The restrictive

147. *Id.*
148. *Id.*
149. *Id.* at 232.
150. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).
151. *See* 5 U.S.C.A. § 552(b)(4) (West 2006).
152. Pub. Citizen Health Research Group v. FDA, 704 F.2d 1280, 1289 (D.C. Cir. 1983).
153. *Id.* at 1288. Commentators have expressed concerns regarding the government's ability

definition "incorporates a direct relationship between the information at issue and the productive process," and thereby properly allowed for the disclosure of information deemed to be worthy of disclosure in the public interest and under the intent of FOIA.[154] It is this type of definition which more closely mirrors the values of openness and transparency found in the ideal democratic government.[155] Similar publicly oriented values should exist with respect to public infrastructure, if public infrastructure is to remain subject to unfettered public inspection.[156]

Building on this analysis, it is clear that trade secrecy is not a doctrine that fits well in government or applies well to those engaged in the provision of public infrastructure traditionally provided by governments. Each element of trade secrecy, whether it be secrecy itself or "commercial use," and the effects of maintaining a secret, whether it be its possible unlimited duration or the possibility of hoarding information that might be

---

to disclose, either accidentally or purposefully, commercial trade secrets that it controls because of its regulatory, contracting, and licensing capabilities. *See generally* Stephen R. Wilson, *Public Disclosure Policies: Can a Company Still Protect Its Trade Secrets?*, 38 NEW ENG. L. REV. 265 (2004) (discussing whistleblower protection and other laws that encourage public disclosure of commercial information, often over the concerns regarding trade secrecy).

154. *Pub. Citizen Health*, 704 F.2d at 1288-89 (adopting a definition of a trade secret, for purposes of FOIA, "as a secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort"); *see also* Dianna G. Goldenson, *FOIA Exemption Five: Will It Protect Government Scientists from Unfair Intrusion?*, 29 B.C. ENVTL. AFF. L. REV. 311, 330 (2002) (noting the difficulties that government scientists face of "unfair intrusion into their scientific process—an intrusion not suffered by scientists in the private sector because those individuals are not vulnerable to disclosure requests under FOIA").

155. It is worth noting that recent scholarship endorsing the notion of a common, open system of infrastructure also illustrates this disconnect. Championed by numerous writers and philosophers, these theories generally examine the theoretical disconnect between operating community resources under restrictive intellectual property rights and the social and societal values that support and encourage the sharing of information. While beyond the scope of this Article, the notion of public infrastructure as a "commons" elevates the various societal benefits that are advanced by emphasizing openness, rather than secrecy. *See* LAWRENCE LESSIG, THE FUTURE OF IDEAS 19-23 (2001) (arguing that there are benefits to holding resources as a commons, with the Internet being the prime example, but noting that there must be a balance between private and public rights); Yochai Benkler, *Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production*, 114 YALE L.J. 273, 275-76 (2004) (analyzing "social sharing" and "shareable goods," and the benefits of applying such ideas and principles to "the domain of sharing rival material resources in the production of both rival and nonrival goods and services"); Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 918-19 (2005) (examining the economics of managing infrastructural resources in an openly accessible manner); Love & Hubbard, *supra* note 118, at 221-23 (discussing alternate methods of financing public goods and noting the benefits of "data transparency").

156. As one commentator has noted, control and sharing are ultimately at odds in trade secrecy doctrine. James W. Hill, *Trade Secrets, Unjust Enrichment, and the Classification of Obligations*, 4 VA. J.L. & TECH. 2, 74-76 (1999). Akin to the battles over defending the public domain, trade secrecy shares this theoretical conflict.

valuable to the public but not the private sector, stand in stark contrast to what we expect, at least in theory, from democratic institutions. More specifically, these values differ from what we should expect from entities that take on governmental roles by seeking the financial rewards of providing essential public infrastructure.

Because these guiding principles influence how trade secret law is applied and what is deemed appropriate in a given circumstance, they must be reconciled if trade secrecy is to have any place in public infrastructure. However, reconciling these divergent values in the context of public infrastructure is nearly impossible if any semblance of maintaining a commercial secret is to be maintained. Moreover, the practical effects of applying trade secrecy law to public infrastructure mean that such reconciliation, even were it possible, is not a good choice. As discussed below, because of these practical considerations, the better option is to severely limit, or eliminate entirely, the application of the doctrine in this context.

3. Concerns When Applying Trade Secret Law to Public Infrastructure

To fully understand the examples in Part V and identify the real effects of this problem, it is useful to consider the practical benefits and drawbacks of elevating transparency and accountability over trade secrecy. Aside from the underlying theoretical conflict that sets these doctrines in opposition and requires that public values be elevated to at least an equal footing with those of commerce, the practical effects of this tension underscore the consequences of this mismatch. The benefits to businesses of having trade secrets were outlined in Part III, and because of the legitimate reasons for maintaining trade secrecy in the commercial context, an argument that such protection should be limited or eliminated requires an examination of the possible benefits of disclosure both to the public and to businesses. Even on a practical level, the benefits of disclosure to the public outweigh the interests of businesses in trade secrecy for the provision of public infrastructure.

Recent history demonstrates that when government has been responsible for the provision of public infrastructure, it has engaged in sweeping and candid discussion, with full information, of policy alternatives and means to achieve infrastructural goals. Consider the building of the Verrazano Narrows Bridge in the 1950s, connecting the New York City boroughs of Staten Island and Brooklyn. Various governmental agencies, public officials, business, and public advocates engaged in a heated debate about the nature of the project.[157] Debated

157. *See* Jon J. Lines & Ellen L. Parker, *The Politics of Infrastructure: Robert Moses and the Verrazano Bridge*, *in* PUBLIC INFRASTRUCTURE PLANNING AND MANAGEMENT 165, 165-88 (Jay

issues included funding, functions, and interaction with other public works projects.[158] Studies were conducted, public and business advocates were consulted, elected officials (like Governor Harriman) and heads of regulatory agencies (including the legendary Robert Moses, who was, at that time, the chairman of the Triborough Bridge and Tunnel Authority (TBTA)) weighed in with arguments and counter-arguments, testimony was given before legislative committees, and *The New York Times* editorialized.[159] Indeed, Robert Moses wrote of his concerns about the "moral right" of the TBTA to spend taxpayer dollars on the project.[160]

The key, according to the authors of an analysis of these events, was that the "political interaction among organizations [had] a decisive impact on infrastructure planning."[161] Such informed debate infused with public discussion and consideration by multiple interested parties is difficult, at best, to conduct when some or all of the very information needed for such discussion is held by private actors and shielded from public view. Because trade secrecy could perpetually impede public disclosure of much information, the very possibility that the public would ever know what is being considered by the government, or how such decisions are reached, is dubious. Meaningful public debate, and the resultant benefits of full and informed consideration of options and alternatives, is suppressed.

Aside from foreclosing meaningful debate and discussion, secrecy can engender distrust and suspicion that is counter-productive for businesses and its customers. Because we rely so heavily on public infrastructure, secrecy becomes especially dangerous. As discussed in Part V, secrecy means that we must guess at how elections are run, who can read our email, and how data is transmitted through the Internet. Absent information, these conditions can create paranoia because guesswork replaces real and verifiable information. The public is left in the dark. The late Senator Daniel Patrick Moynihan, in his excellent historical analysis of secrecy as a form of government regulation, explained that the conflict created by such a scenario is akin to "[i]gnorant armies clash[ing] by night."[162]

The result is that the public may worry about issues that, with adequate information, could be discarded (or confirmed) as trivial (or real) concerns. Potentially wasting energy and resources, the public under our current system must choose between trust by faith and suspicion by ignorance. While many people may not give this issue much thought, it is

M. Stein ed., 1988).

158. *See id.*

159. *See id.*

160. *Id.* at 180.

161. *Id.* at 187.

162. Richard Gid Powers, *Introduction* to DANIEL PATRICK MOYNIHAN, SECRECY 1, 16 (1998) (quoting Moynihan and discussing at length the benefits to society of less governmental secrecy).

difficult to ignore such concerns because we interact with this infrastructure—roads, the Internet, governmental actions like law enforcement—on a daily basis. In the absence of adequate information, the public regularly uses infrastructure with limited or no knowledge as to how it operates and how that form of operation impacts our daily lives.

Whether motivated partly by paranoia or not, the existence of public watchdog websites like votersunite.org suggests the impact that secrecy has on public confidence.[163] This website reports on, among other topics, election irregularities and the operation of voting machines, and it encourages public efforts to change the election process.[164] It states:

> The abundance of practical problems with electronic voting is not the fundamental violation of our democracy. The fundamental violation is that when computers are used to record and count votes, ordinary people cannot observe the process. For a democracy to thrive, all citizens must be able to observe the casting of their ballots and the counting of their votes, not just observe computers processing their votes in secret.[165]

While this may seem to be an extreme position, and it is possible that such websites would exist even if information were made public, there can be no doubt that when Diebold refuses to make public the inner workings of their voting machines, they feed the very concern that causes such a website to exist. From a consumer confidence perspective alone, Diebold would likely do better by not reinforcing these concerns.[166]

This problem is further compounded because maintaining such secrecy evinces a lack of trust in the public, and in the case of items sold directly to the government, like voting machines, in the government as well. While businesses have often expressed legitimate concern about inadvertent disclosure of trade secrets entrusted to the government as part of the

163. *See* Voters Unite!, http://www.votersunite.org/about.asp (last visited Oct. 16, 2006).

164. *See* Voters Unite!, http://www.votersunite.org/takeaction.asp (last visited Oct. 16, 2006).

165. *Id.*

166. This is merely one of several such websites dedicated to examining voting systems and irregularities, and pressuring election officials and machine manufacturers to disclose information and improve the election process, or both. *See, e.g.*, Black Box Voting, http://www.blackboxvoting.com (last visited Oct. 16, 2006); California Voter, http://www.calvoter.org/news/blog/index.html (last visited Oct. 16, 2006); Election Science Institute, http://www.electionscience.org/ (last visited Oct. 16, 2006); North Cardina Coaltion for Verified Voting, http://www.ncvoter.net/ (last visited Oct. 16, 2006); Verified Voting, http://www.verifiedvoting.org/ (last visited Oct. 16, 2006); Where's the Paper Trail?, http://www.wheresthepaper.org/ (last visited Oct. 16, 2006). Also, a recent documentary on Home Box Office entitled "Hacking Democracy" demonstrates the concerns of citizens voting in an election process shrouded in secrecy.

regulatory process,[167] when the consuming public seeks basic information about its own infrastructure, businesses' reaction should be different. By taking the position that their trade secrets cannot be disclosed to a public that uses and, in one form or another, pays for such infrastructure and seeks to verify that it is working as it should, people may logically conclude that there must be something to hide.

While there may be good business reasons for secrecy, such as maintaining competitive advantages and capturing the value of innovations, the legitimate concerns of the public should outweigh commercial necessity. The business needs of a company fail to assuage a public that is fighting to access basic information about its infrastructure's operations. More importantly, the public at large should not be treated as a competitor from whom valuable information should be denied. Rather, in these contexts, the public is a consumer who wants and needs to know what they are using to vote, communicate, and live life. The lack of trust in the public—perceived or real—undermines the credibility that any business would want to enjoy from its consumers.

The potential for increased confidence displayed by consumers in a forthcoming company may lessen the sting of losing trade secrecy protection. Beyond the damaging effects to public relations and confidence of merely asserting that information should be secret, the poor fit of commercial trade secrecy and public infrastructure manifests itself in more concrete ways. A trade secret may be hoarded and kept forever—eliminating the possibility that the secret could be examined, shared, or improved upon by the public unless expensive or illegal steps, like reverse engineering or misappropriation, respectively, are taken to undermine trade secret protection.[168] This condition makes theoretical sense in the commercial world because, among other reasons, unfair competition (like stealing a trade secret) violates general norms of ethical business conduct and keeping certain information secret from competitors is often believed (rightly or wrongly) to be a prudent business decision.[169] Trade secrecy's application in the public sector, on the other hand, makes little sense where profit is not a concern, but accountability through transparency is. This problem is made obvious by the fact that under current law, Diebold may *never* have to affirmatively reveal its source

167. *See supra* note 153 and accompanying text.

168. *See supra* Part III.B.3. This is one of the many factors that distinguish trade secrets from patents, an arguably more "democratic" concept, and a topic explored more fully in Part VI.

169. Of course, time and effort are potentially wasted because duplicative research can occur when one does not know what others are doing. That, however, is the commercial trade-off in trade secrecy: The risk of duplicative effort is outweighed by the commercial advantage of maintaining the secret. Considering the limited resources already applied to public infrastructure, *see supra* note 32 and accompanying text, duplicative research and wasted effort should be minimized in this context as much as is possible so as to maximize output in this underfunded sector of our society.

code[170] to a public that relies upon it for the proper functioning of legal elections and that may want to improve the operation of the elective process beyond what is profitable to Diebold.

Additionally, the existence of the right to a perennial secret might make sense in the commercial context where the owner of the secret runs the risk of it being reverse-engineered or independently discovered. But, it also creates incentives to aggressively guard against public disclosure, which again forces the public into an informational darkness about infrastructure. For example, to get the benefit of potentially infinite protection from public disclosure (and indeed, any other benefit of trade secrecy), one must meet the elements of a trade secret in the states in which the product might be used or disclosed, including the most extensive requirements to maintain secrecy.[171] Thus, because trade secret law is created by state laws as opposed to one federal law, at least one commentator has noted that the business incentive might be to adopt a confidentiality program that meets the requirements of the most restrictive state in which the information may be used or disclosed.[172]

In the technological sector, the possibility of maintaining a trade secret infinitely can lead to such incentives as purposely designing awkward and cumbersome computer protocols in order to raise the cost and decrease the possibility of reverse engineering.[173] While one could legitimately question the actual likelihood of a trade secret never being revealed, independently discovered, or reverse engineered in a given situation, the more-than-100-year existence of the Coca-Cola formula trade secret renders the possibility of an infinite trade secret more than theoretical.[174] Thus, if maintained as trade secrets, the public could never have access to the operational underpinnings of voting machines or the telecommunications system they use to communicate with the government, businesses, and each other.

Furthermore, one of the major drawbacks of trade secrecy is discouraging cooperation between businesses. While a business may license a trade secret to another, licensing is a long way from free access to information and the ability of the public to offer criticisms or suggestions for improvement. The continued core of trade secrecy is

170. "A computer program's source code is the collection of files that can be converted from human-readable form to an equivalent computer-executable form." Wikipedia, Definition of Source Code, http://en.wikipedia.org/wiki/Source_code (last visited Oct. 15, 2006). Source code allows a computer to operate and perform the program's functions. *See id.*

171. *See* Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427, 446 (1995).

172. *See id.* at 446-47.

173. *See* Douglas Lichtman, *Property Rights in Emerging Platform Technologies*, 29 J. LEGAL STUD. 615, 633-34 (2000) (noting that, in the context of platform technologies like desktop computers or operating systems, current intellectual property law encourages developers to create complex, rather than simple, processes and programs).

174. *See supra* note 91 and accompanying text.

implied, i.e., the doctrine was not designed to encourage cooperation or sharing of information, but to prevent it in order to preserve competitive advantages between businesses.[175]

Cooperation can also create the apparatus to allow for improvements in the provision of public infrastructure by way of public deliberation. Jon Elster has written about the positive effects of public deliberation on the conduct of the public's representatives in government.[176] Defined as the "civilizing force of hypocrisy," Elster explains that "[g]enerally speaking, the effect of an audience is to replace the language of interest by the language of reason and to replace impartial motives by passionate ones."[177] Similarly, the effect of forcing public infrastructure providers to have their products and services discussed in a public forum would, at least arguably, force these private providers to implement improvements and foster in them more appreciation of the public roles that they have engaged. At a minimum, it would create an atmosphere in which the public's judgment of the merits of a particular good or service could not be easily ignored.

While one could argue that if society wants to reap the benefits (whatever they may be) of a private entity providing public infrastructure then it must pay some of the price (like allowing that entity to turn a profit by standard commercial means and tactics), it cannot be that these commercial entities can simply conduct their business without reference to the responsibilities that should become their burden.[178] To hold

175. Brett Frischmann, in a talk at the Center for Internet and Society at Stanford Law School regarding his economic theory of infrastructure, noted that sharing may benefit private businesses and that it is not always the case that sharing would result in lost value. *See* Brett M. Frischmann, Lecture at the Stanford Law School Center for Internet and Society: An Economic Theory of Infrastructure (and a Normative Argument for Promoting Sustainable Infrastructure Commons) (Mar. 8, 2004), *available at* http://cyberlaw.stanford.edu/events/archives/brett_m_frischmann.shtml (follow "Listen to Professor Frischmann's talk" hyperlink). In his opinion, businesses need to be educated as to where such benefits might reside. *Id.*

176. John Elster, *Deliberation and Constitution Making*, *in* DELIBERATIVE DEMOCRACY 97, 111 (Jon Elster ed., 1998).

177. *Id.* While beyond the scope of this Article, Elster's detailed explanation of this notion is an extremely thought-provoking and practical analysis of the positive effects of public deliberation in recent social science scholarship.

178. *See* LESSIG, *supra* note 155, at xviii (disapproving of former Federal Communications Commission Chairman Michael Powell's argument that there was an economic need to give cable operators free reign over "their property" if they were going to invest in building the "infrastructure of the information superhighway"). If these operators chose to discriminate over what could be done on their resource, Powell argued, such was the price to pay for their investment. *Id.* Indeed, the United States Supreme Court has found that public and private interests can become so enmeshed that the private entity's actions are imputed to the public entity. *See* Burton v. Wilmington Parking Auth., 365 U.S. 715, 716-17, 725 (1961) (involving a pre-Civil Rights Act issue in which a privately-owned restaurant, leasing space in a publicly-owned building, refused to serve an African-American, and holding that the "State has so far insinuated itself into a position of interdependence with [the restaurant] that it must be recognized as a joint participant in the challenged activity" and finding the State in violation of the Fourteenth Amendment). It stands to

otherwise would be to allow businesses to conduct public business, and, for all practical purposes, mimic roles normally played by government, without taking on the responsibilities of a public actor.

Additionally, allowing the providers of public infrastructure to set the terms of the public's interaction with their products and services, which in the instances described below is in fact what is happening, moves society into the realm of "code as law," as articulated by Lawrence Lessig.[179] The choice of "modalities of regulation," such as law, norms, architecture, or the market, determines what values are emphasized.[180] When the modality of regulation adheres to the values that, as a society, we believe should exist in the product or service, then this phenomenon is of marginal concern. However, in the present context, regulation is thrust upon the public by the private sector through its very provision of infrastructure. Businesses are making the decisions, often without much public input or involvement, as to the nature, scope, and capabilities of our public infrastructure. Backed by notions like trade secrecy, this public infrastructure—and its "code"—embodies not public, but commercial values.

As Christoph Engemann has noted in the context of voting machines, "If the code gains regulatory power and is meant to contribute to the public good it needs to be accessible and disputable just like the law is readable and disputable (at least by lawyers[])."[181] To allow public infrastructure to be provided without public debate ultimately undermines democracy by frustrating that basic tenet. Code developed by the private sector, at least in the United States, has indeed become regulatory: "Code" is our public infrastructure, is stifling public access to information and informed debate about how our public infrastructure should operate, and is in many cases entirely inaccessible and therefore indisputable.

What is clear is that businesses are, in significant respect, governing in the public sense. They are providing a public service by providing public infrastructure, often in the place of government. But they are also economically benefitting, reaping profits and opening markets previously foreign to private industry. Therefore, in these instances, they should take on certain governmental responsibilities and observe certain public duties,

---

reason that the converse should be true: Private entities can become so enmeshed in public activities, like providing municipal wireless Internet access, or governmental functions, like manufacturing and selling voting machines, or both that they should be held to a higher standard of responsibility akin to that of the government to the public.

179. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (outlining and analyzing the phenomena in the Internet realm that allow code—the software and hardware that forms cyberspace—to dictate the nature and freedoms inherent in it).

180. *See* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 686-87 (1998) (noting how different modes of regulation may produce and displace certain values).

181. Posting of Christoph Engemann to Engemann Blog, http://cyberlaw.stanford.edu/blogs/engemann/archives/003663.shtml (Dec. 5, 2005, 7:07 PST).

like informing the public of their operations and activities. This trade-off recognizes the fact that in a commercial market the public will often pay (in one form or another) for these services, but that it has a right to disclosure when companies supplant or replace government in the role of provider.

As discussed above, abandonment of secrecy as a business strategy may also benefit the businesses themselves, even were trade secrecy displaced by other more democratic forms of commercial protection, like patent.[182] In the end, given the extremely expansive nature of modern trade secret law, the application of the law to the public infrastructure scenario must change if we wish to retain any notion of public participation in the process that creates and maintains our public infrastructure.

V. THE CONFLICT AS IT EXISTS TODAY

Because of notions like reverse engineering and independent discovery, trade secrecy law is often considered a relatively weak source of protection for business, as compared to copyright and patent. However, the scenarios below suggest that in the public infrastructure context, the law is more powerful than previously believed. It is in the practical manifestation of these conflicts that the true dichotomous elements of trade secrecy and government values are illustrated, and in the ensuing quarrel, secrecy wins; transparency and accountability are consistently on the losing end. By examining three representative scenarios, it becomes apparent that public infrastructure operates in the shadows. The import of the information hidden from view is remarkable, and requires a significant change in the law.

A. *Example One:* Cisco Systems Inc. v. Michael Lynn

Take, as a first example, the operations of the Internet—an increasingly essential public infrastructure used by both government and the global public. In the summer of 2005, Michael Lynn (Lynn) was asked by his employer, Internet Security Systems, to reverse engineer Cisco Internet Operating System (IOS), the operating system running Cisco Systems' (Cisco) routers owned by private and public entities.[183] Based upon that

182. *See infra* Part VI (analyzing the tradeoff to businesses and the potential impact of abandonment).

183. "A router acts as a junction between two networks to transfer data packets among them." *See* Wikipedia, Definition of Router, http://en.wikipedia.org/wiki/Router (last visited Oct. 14, 2006). While one could question whether a privately-owned router is part of public infrastructure (a topic that I intend to explore in a future project on the modern definition of public infrastructure), there is no dispute that routers are fundamental to the orderly operation of the Internet. As Cisco noted in a press release announcing a new product created in an alliance with Fujitsu, "Networks have become lifelines for public infrastructure and corporate IT systems, leading to ever-increasing

research, Lynn planned to reveal a security vulnerability in Cisco's routers to Black Hat, a conference of computer security experts and hackers.[184] The security vulnerability, known as "exploit code," demonstrated an ability to remotely execute code on Cisco routers, thereby controlling and taking over the operation of the router.[185]

While Cisco had corrected the flaw and stopped distributing computer code that would allow for this exploit to work, Lynn believed that Cisco did not do enough to encourage its customers to correct the problem by upgrading the software on their routers, and that it had not explained why this was necessary.[186] In response to Lynn's employer's instructions not to give the presentation, Lynn quit his job and planned the presentation anyway.[187] Significantly, however, the planned presentation did not reveal sufficient information for one to recreate the "exploit code" without, at best, "a lot of work."[188]

Upon hearing of the planned presentation, Cisco quickly brought an action against Lynn and Black Hat. It sought, among other relief, an injunction against Lynn giving the presentation and thereby disclosing Cisco's alleged trade secrets.[189] Cisco argued, in part, that Lynn and Black Hat violated California's trade secrets law[190] by misappropriation because Cisco's trade secrets were "acquired improperly through the breech [sic] of an agreement to keep them secret."[191]

The result: Lynn settled with Cisco.[192] The terms of the settlement were

---

requirements for quality and reliability." Press Release, Fujitsu Ltd. & Cisco Sys., Inc., Fujitsu and Cisco Deliver Next-Generation High-End Routers Based on Strategic Alliance (May 24, 2005), *available at* http://www.internetadsales.com/modules/news/ article.php?storyid=5630. Thus, as such routers serve as a vital piece of networking equipment that allows for access to all corners of the Internet, I submit that they constitute part of our public infrastructure.

184. Kim Zetter, *Router Flaw Is a Ticking Bomb*, WIRED, Aug. 2, 2005, http://www.wired.com/news/politics/0,68365-0.html.

185. *See* Posting of Jennifer Granick to The Shout: Opinions on Everything, http://www.granick.com/blog/archive/2005_08_01_theshout_archive.html#112302921362405957 (Aug. 2, 2005, 17:28 PST). Jennifer Granick, Executive Director of Stanford Law School's Center for Internet and Society, represented Lynn in the ensuing litigation.

186. *Id.*

187. *Id.*

188. *Id.* Indeed, Granick asserts that Lynn did not even possess secret "source code," but rather "binary code" that is actually sold by Cisco. Posting of Jennifer Granick to The Shout: Opinions on Everything, http://www.granick.com/blog/archive/2005_08_01_ theshout_archive.html# 1123118061797688898 (Aug. 3, 2005, 18:10 PST).

189. Complaint at 7-8, Cisco Sys., Inc. v. Lynn, No. 05-CV-03043 (N.D. Cal. Jul. 27, 2005), *available at* http://www.eff.org/Activism/E-voting/McCloy_amended_complaint.pdf.

190. CAL. CIV. CODE §§ 3426-3426.11 (West 2006).

191. Complaint, *supra* note 189, at 6.

192. While Granick was confident that Lynn could have defeated the trade secrets claim because (a) the subject code was not actually secret, (b) reverse engineering is allowed under California law, and (c) this claim was more akin to a breach of contract action than misappropriation of a trade secret, she believed that it was in the interest of Lynn to settle rather

broad and effectively ended any further dissemination of this information. Lynn agreed, in part, to be enjoined from "disclosing or disseminating" the information, reverse engineering Cisco's code, and using the code "for any purpose."[193] Additionally, Lynn agreed to identify to whom, if anyone, he disclosed the alleged trade secrets, and return the fruits of his labor to Cisco's counsel, who would eventually destroy the data.[194]

Given Cisco's router production dominance, the settlement effectively ended the public dissemination and informed discussion of these potential security vulnerabilities (by one measurement, Cisco had 55.7% of the Internet's "big router" market).[195] That Cisco could bring a trade secret misappropriation action under such circumstances, and force parties to litigate or enter into agreements to maintain the secrecy of security information is, I propose, a superb example of the problem with the current law. California's broad definition of a trade secret, which tracks the expansive definition found in the UTSA,[196] at least arguably covered the subject information and made the question of whether this information was covered by the law subject to some dispute.

The result of bringing this action rendered difficult, if not impossible, any further examination or informed discussion of this potential problem as identified by Lynn, who spent time seeking to understand the issues and its ramifications for the benefit of the public. Information regarding the operations of a basic element of the Internet that could be used to compromise it was protected as a secret. Such information should be made public, especially in the absence of a public solution to the problem, because the potential impact of a major failure of these routers would shut down much of the Internet, a major public infrastructure.

The fact that it was Lynn, an individual unauthorized by Cisco to examine the routers, who identified and exposed this problem, underscores the need for the public—and not certain limited individuals chosen by government or even watchdog groups—to have access. To allow chosen individuals, whether the government or third-party escrow agents, limited access puts undue power in the hands of the party selecting the lucky few,

---

than fight because the terms of the settlement required Lynn to do things that he was, for the most part, willing to do anyway. *See* Granick, *supra* note 188. The logical and, from her client's perspective, proper goal was to "get out of the case as unscathed as possible." *Id.*

193. Stipulated Permanent Injunction at 1-2, Cisco Sys., Inc. v. Lynn, No. 05-CV-03043 (N.D. Cal. July 28, 2005), *available at* http://www.siliconvalleysleuth.com/files/stipulated_permanent_injunction.DOC.

194. Stipulated Permanent Injuction, *supra* note 193, at 3-4.

195. Scott Moritz, *Cisco Maintains Router Lead on Juniper*, THESTREET.COM, Aug. 18, 2005, http://www.thestreet.com/pf/tech/scottmoritz/10238750.html (last visited Oct. 16, 2006). "[B]ig routers" are the hardware "used at central junction points to direct data traffic." *Id.* That Cisco's routers may ultimately be purchased by governments and used in the operation of public infrastructure underscores the need for reexamining trade secrecy's application.

196. *See* CAL. CIV. CODE § 3426.1(d) (West 2006).

and even more power in the hands of those who control the information. The next Lynn might be someone no person in power knows; and her contribution could be significant.

More significantly, the public's right to access this information was completely subjugated to the marginal claim that some of this information might qualify as a trade secret. The chilling effect of such claims, including the need for a defendant to expend time and energy litigating, makes settlement a reasonable choice in many circumstances. In this case, it also meant that this information remained subject to laws designed to protect Cisco's interest, not the public's. In fact, it could deter the uninformed from future efforts to access such information by reverse engineering for fear of somehow violating the law. At the end of the day, the law contributed to forcing a settlement that kept crucial information away from the public, about an infrastructure that is now, in many respects, the backbone of public infrastructure.

B. *Example Two: Voting Machines and Diebold Election Systems, Inc.*

As a second example, consider Diebold's provision of voting machines to certain states. Diebold has repeatedly refused to reveal source code used in the operation of its voting machines for public inspection to assure the company's suitability to conduct accurate elections.[197]

In November 2005, Diebold refused to comply with a North Carolina law that requires vendors of electronic voting machines to place, among other items, "all software that is relevant to functionality, setup, configuration, and operation of the voting system," including its source code, "in escrow with an independent escrow agent approved by the State Board of Elections."[198] The law is designed to "restore public confidence in the election process" by requiring that such information be provided to the state so as to support and test voting systems.[199] In the ensuing action brought by Diebold against the North Carolina State Board of Elections (BOE) to seek a temporary restraining order and preliminary injunction against the enforcement of the statute,[200] Diebold alleged that it could not

197. The United States Government Accountability Office has recently noted that "security and reliability" remains a concern for "electronic voting systems." U.S. GOV'T ACCOUNTABILITY OFFICE, ELECTIONS: FEDERAL EFFORTS TO IMPROVE SECURITY AND RELIABILITY OF ELECTRONIC VOTING SYSTEMS ARE UNDER WAY, BUT KEY ACTIVITIES NEED TO BE COMPLETED 2 (2005). *See infra* note 206.

198. N.C. GEN. STAT. ANN. § 163-165.9A(a)(1) (West 2006).

199. General Assembly of North Carolina, 2005 N.C. Sess. Law 323, 323 (West).

200. Memorandum of Points and Authorities In Support of Motion to Modify or Vacate Temporary Restraining Order at 1-2, Diebold Election Sys., Inc. v. N.C. State Bd. of Elections, No. 05-CVS-15474 (N.C. Super. Ct. Nov. 16, 2005), *available at* http://www.eff.org/Activism/E-voting/20051117_Diebold_v_NC_Motion.pdf.

provide some of the required information because the information belonged to third parties, and thus was not controlled by, or in the custody of, Diebold.[201] Consequently, Diebold alleged that it could not submit a vendor proposal meeting all state law requirements without "being in violation of state law."[202]

The court eventually held, in essence, that Diebold must comply with the law if it wanted to do business with the state.[203] Diebold responded, however, that it could not disclose source code because of license agreements, and because some of the code belonged to third parties who would be unwilling to disclose it.[204] After another round of court battles, which ensued after the BOE approved Diebold (notwithstanding its inability to comply with the law), Diebold chose not to do business with the state.[205]

That trade secret law or principles of secrecy or both are at play here, even if not explicitly stated, is confirmed by Diebold's explanation to the BOE that "we believe it is impossible for any vendor of an election system to say that they have access to all of the source code in question or that it is all in escrow somewhere."[206] This is a true Pyrrhic victory: Although the state won the initial court battle, the power of trade secrecy principles

201. Complaint at 6-8, 10, Diebold Election Sys., Inc. v. N.C. State Bd. of Elections, No. 05-CVS-15474 (N.C. Sup. Ct. Nov. 4, 2005), *available at* http://www.eff.org/Activism/E-voting/diebold_complaint.pdf.

202. Complaint, *supra* note 201, at 10.

203. Gary D. Robertson, *N.C. Judge Declines Protection for Diebold*, ABC NEWS, Nov. 28, 2005, http://abcnews.go.com/Technology/wirestory?id=1354023; *see also* Order of Dismissal at 1, Diebold Election Sys., Inc. v. N.C. State Bd. of Elections, No. 05-CVS-15474 (N.C. Sup. Ct. Nov. 30, 2005), *available at* http://www.eff.org/Activism/E-voting/diebold_order_dismissal.pdf.

204. Anne Broache, *North Carolina Defends E-Voting Certifications*, CNETNEWS.COM, Dec. 2, 2005, http://news.com.com/North+Carolina+defends+e-voting+certifications/2100-1028_3-5980671.html?tag=mainstry (last visited Oct. 16, 2006).

205. Letter from Charles R. Owen, Div. Counsel, Diebold Election Sys., Inc., to Gary Bartlett, Executive Dir., N.C. State Bd. of Elections (Dec. 20, 2005), *available at* http://www.votetrustusa.org/pdfs/Diebold%20Folder/Barrett%20Letter%2012-21-05-1.pdf; *see also infra* note 211 and accompanying text.

206. Letter from Charles R. Owen to Gary Bartlett, *supra* note 205, at 1. Diebold has argued that such information is akin to trade secrets in other cases. *See* Response to Plaintiffs' Post Hearing Letter and Supplemental Declaration, and Request for Early Status Conference or Reference to Mediation at 3, Online Policy Group v. Diebold, Inc., No. 03-4913JF (N.D. Cal. Nov. 24, 2003), *available at* http://www.eff.org/legal/ISP_liability/OPG_v_Diebold/DieboldResponse.pdf (noting that "Diebold has informally encouraged the students to refrain from publishing passwords, source codes, information protected by employees' privacy interests and trade secret-type information, none of which is essential for purposes of criticism."); Joseph Lorenzo Hall, Transparency and Access to Source Code in Electronic Voting 9 (unpublished paper), *available at* http://www.usenix.com/events/evt06/tech/full_papers/hall/hall.pdf (noting that voting machine vendors have asserted trade secret protection over their software). Of course, as discussed above, access to source code is essential for understanding how a voting machine operates. *Id.* at 3 (noting that "[a]ccess to source code supports independent technical evaluation of voting systems that, in turn, facilitates oversight and accountability of software").

presumably remained, because protection of secrets was not overruled or overridden by the concerns of the public as manifested by the laws of the state. Thus, Diebold could focus on states where trade secrecy law is completely impermeable to public-law overrides.

More recently, computer hackers successfully broke into Diebold's voting machines owned by Leon County, Florida to test their vulnerability to manipulation. What made this event particularly unusual was that the hackers were given access to the Diebold machines by Leon County Supervisor of Elections Ion Sancho.[207] Diebold's response to being informed of four successful hacks of their machines, which one hacker likened to "prestuffing a ballot box," was to say that these tests were "invalid" and "potential violations of licensing agreements and intellectual property rights."[208] Sancho replied that "[m]ore troubling than the test itself was the manner in which Diebold simply failed to respond to my concerns or the concerns of citizens who believe in American elections."[209] Identifying the heart of the problem, Sancho also lamented, "I really think they're not engaged in this discussion of how to make elections safer."[210]

It is difficult to find a more fundamental public infrastructure than a voting machine. Sadly, however, even when the very ability to conduct an accurate and verifiable election is at issue, trade secrecy wins the day. Secrecy supported by the law resulted in a private actor being able to argue against traditional governmental notions of transparency and accountability and disengage from public discussion about proven vulnerabilities of their products. True, one could conceive lawful ways to access this trade secret information in the absence of contractual prohibitions, like reverse engineering. But the fact that legislatures have to pass laws mandating that source code about voting machines must be available to the state, and state boards of elections and officials charged with operating fair and accurate elections have to jump through such legal hoops (and may not be successful in doing so) reflects a balance that is skewed in favor of commercial interests and against those of the public. The risk of being able to prestuff a ballot box was not enough for Diebold to concede that public disclosure of the inner workings of the machines

207. Zachary Goldfarb, *As Elections Near, Officials Challenge Balloting Security*, WASH. POST, Jan. 22, 2006, at A6, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/01/21/AR2006012101051.html.

208. Marc Songini, *Q&A: E-Voting Systems Hacker Sees 'Particularly Bad' Security Issues*, COMPUTERWORLD, Jan. 19, 2006, http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,107881,00.html.

209. *See* Goldfarb, *supra* note 207.

210. *See id.* Diebold, and two other voting machine vendors, apparently now refuse to deal with Leon County, which has prompted the Florida Attorney General to issue subpoenas to those companies. Marc Songini, *Florida Attorney General Questions E-Voting Vendors' Decision to Shun County*, COMPUTERWORLD, Apr. 4, 2006, http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,110192,00.html.

might be appropriate, even if for no other reason than to prove that it took the issue seriously and had nothing to hide from the public. The law must step in to force such change.

Moreover, one significant additional element in the Diebold-North Carolina scenario underscores the inability of government to always be a third-party ombudsman for, or protector of, the public's interest. As mentioned earlier, immediately after Diebold refused to comply with the law, and in the face of their refusal to do so, the BOE in effect nullified the law and actually *approved* Diebold as a vendor, noting that none of the winning applicants could comply with the law's requirement that all source code be placed in escrow.[211] Moreover, a court challenge to that decision was unsuccessful,[212] and, ultimately, the only fact that prevented the use of Diebold's machines in North Carolina was Diebold's decision to withdraw from the state. Suggesting that this is a law that can be followed and that businesses might serve a market in which trade secrecy is not sacrosanct, rival vendor Election Systems & Software agreed to comply with the state's law. [213]

Thus, aside from trade secrecy law defeating the disclosure law in practice, the notion that a government-controlled or designated entity could adequately protect the interests of the general public is dubious, and would turn on many variables that might undermine the third party's ability to operate in a completely public-oriented fashion. Indeed, where a state agency effectively nullifies a law designed to protect the public's interest, the entire basis upon which an escrow regime would be built—that is, trusting the entity charged with examining the escrowed material—is undermined. Thus, it is not readily apparent that a third-party (governmental or otherwise) might adequately protect the general interests of the public.[214]

C. *Example Three: Citywide Wireless Internet (Wi-Fi)*

One of the major public infrastructure goals of many municipalities is to provide high-speed Internet access to all of its residents. President

211. Broache, *supra note* 204; *see also* Amended Verified Complaint for Writ of Mandamus at ¶ 17, McCloy v. N.C. State Bd. of Elections, No. 05-CVS-16878 (N.C. Super. Ct. Dec. 19, 2005), available at http://www.eff.org/Activism/E-voting/mccloy_amended_complaint.pdf.

212. *See* Electronic Frontier Foundation, Litigation, http://www.eff.org/Activism/E-voting/ (last visited Oct. 16, 2006).

213. *See* Electronic Frontier Foundation, After EFF Litigation, Diebold Pulls Out of North Carolina (Dec. 23, 2005), http://www.eff.org/news/archives/2005_12.php.

214. *See* Hall, *supra* note 206, at 6 (noting that it is unclear whether the North Carolina statute will be enforced). While one could argue that my concern is more with government than with the operation of trade secrecy doctrine, it is again the idea that laws must be passed, litigation must be commenced, and extensive effort must be made for companies to reveal such information that makes trade secrecy doctrine problematic in this context.

George W. Bush has mentioned access to "the information that is transforming our economy through broadband technology" by setting the goal of "broadband technology to every corner of our country by the year 2007 with competition shortly thereafter."[215] Democrats in the House of Representatives, led by Rep. Nancy Pelosi, have articulated a similar goal.[216] These goals are being implemented by cities that see citywide wireless networks as helpful to low-income residents by providing access to the Internet, building public-safety networks, connecting city agencies, and aiding economic development by luring people into cities.[217] A brief examination of two cities' efforts, Philadelphia and San Francisco, illustrates the trade secret issues at play.

In July 2004, the city of Philadelphia embarked on the development of a citywide Wi-Fi system by forming a non-profit corporation called "Wireless Philadelphia" to examine the possibility of citywide Wi-Fi and develop a plan for its implementation.[218] It explained in its "Wireless Philadelphia Business Plan" that the basic goal and role of government in the project was to provide "the framework and initial investment needed to fully exploit this opportunity," noting the traditional fact that "the public sector will need to serve as the catalyst to ensure that affordable broadband Internet access is widely available to all the residents of Philadelphia."[219]

After an extensive bidding process, in October 2005 Wireless Philadelphia announced a public-private partnership and chose the company EarthLink to "fund, build and manage" the network; no city tax dollars would be used. In essence, under the plan EarthLink will provide the Wi-Fi infrastructural backbone, and individual Internet service providers will sell access.[220] Significantly, however, Wireless Philadelphia retained some reversion rights to the intellectual property of its potential vendors in its "Request for Proposals for a Citywide Wireless Network"

215. Press Release, White House, President Unveils Tech Initiatives for Energy, Health Care, Internet (Apr. 26, 2004), *available at* http://www.whitehouse.gov/news/releases/2004/04/20040426-6.html.

216. *See* Anne Broache, *Democrats Unveil 'Innovation Agenda,'* CNETNEWS.COM, Nov. 15, 2005, http://news.com.com/2100-1034_3-5953520.html (quoting Rep. Pelosi as saying, "Universal broadband—whether it's delivered by Wi-Fi or WiMax, or hard line—will put all Americans, no matter where they live, no more than a keystroke or a mouse click away from the jobs and opportunity broadband both creates and supports . . . .").

217. Marguerite Reardon, *Cisco Enters Citywide Wireless Market*, CNETNEWS.COM, Nov. 15, 2005, http://news.com.com/2100-7351_3-5952090.html.

218. *See* Wireless Philadelphia™ Business Plan presented to Honorable John F. Street, Mayor of Philadelphia, PA 7-8 (Feb. 9, 2005), *available at* http://www.wirelessphiladelphia.org/pdfs/Wireless-Phila-Business-Plan-040305-1245pm.pdf.

219. *Id.* at 9-10.

220. Declan McCullagh, *EarthLink Wins Philly Wi-Fi Contract*, CNETNEWS.COM, Oct. 4, 2005, http://news.com.com/2100-7351_3-5888494.html (quoting Dianah Neff, Philadelphia's chief information officer); *see also* Wireless Philadelphia WI-FI Project Update December 2005, http://www.wirelessphiladelphia.org/pdfs/WP_Update_Dec_2005.pdf.

(RFP). In a clause entitled "Reversion to Wireless Philadelphia," it reserved the right to be "granted all licenses to intellectual property necessary for operation and maintenance of the [wireless system]" in the event of a "material, uncorrected and persistent failure" of the system to meet the terms of the contract with Wireless Philadelphia.[221] Thus, although not apparently requiring that all trade secrets and other intellectual property be made generally available to it, Wireless Philadelphia apparently recognized that it would need access to such information if its vendor did not correct systemic and persistent problems.[222]

Contrast Wireless Philadelphia's process with the current nascent efforts of the city of San Francisco. San Francisco, similar to Philadelphia, has created the TechConnect venture and is seeking to develop a citywide Wi-Fi system that would cost taxpayers "little or nothing," in an effort to promote "digital inclusion" for all of San Francisco's residents. It has sought proposals from potential vendors in the form of a Request for Information and Comment (RFI/C) and a subsequent RFP, but city officials would not detail the contents of any RFI/C, for fear that they may include trade secrets.[223] Moreover, the RFP includes two provisions that provide that the City of San Francisco will make public the complete contents of industry-submitted proposals *except* redacted information that qualifies as a trade secret under California law.[224] Based upon the

221. WIRELESS PHILADELPHIA, REQUEST FOR PROPOSALS FOR A CITYWIDE WIRELESS NETWORK 38, *available at* http://www.wirelessphiladelphia.org/pdfs/WP%20RFP%204-5-05%20rev%20v4-CLEAN.pdf (last visited Oct. 21, 2006).

222. The Wireless Philadelphia Broadband Network Agreement ("Agreement"), executed on February 21, 2006 between EarthLink and Wireless Philadelphia, includes a paragraph entitled "Confidentiality." Wireless Philadelphia Broadband Network Agreement 1, 24-25, *available at* http://www.wirelessphiladelphia.org/pdfs/Network_Agreement_for_PDF.pdf [hereinafter Agreement]. It includes extensive protection for confidential information and trade secrets of EarthLink. Indeed, "confidential information," which cannot be disclosed to third parties except under certain limited circumstances, is defined to include "all information concerning EarthLink, its business plans, pricing, proprietary rights, [s]ubscribers, customers and suppliers." *Id.* While some of this data, like subscriber information, may rightfully be held in confidence, it would appear that EarthLink could attempt to designate a wide variety of information, like information regarding security, as confidential. Indeed, the publicly-released exhibits to the Agreement include three redactions for technical information deemed "confidential and propriety." Agreement, *supra*, at http://www.wirelessphiladelphia.org/pdfs/WP%20EL_Network_Agreement_Exhibits.pdf. It is impossible to determine the import of that redacted information, which is precisely the problem.

223. Stefanie Olsen, *Google Faces Obstacles in S.F. Wi-Fi Bid*, CNETNEWS.COM, Oct. 3, 2005, http://news.com.com/2102-7351_3-5887919.html?; *see also* CITY & COUNTY OF S. F., REQUEST FOR INFORMATION AND COMMENT 2005-07 6 (Aug. 16, 2005), *available at* http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/BroadbandFinalRFIC.pdf; CITY & COUNTY OF S. F., REQUEST FOR PROPOSALS 2005-19 (Jan. 17, 2006) [hereinafter RFP 2005-19], *available at* http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/TechConnectRFP_2005-19_12-22-05Rev1-17-06.pdf.

224. *See* RFP 2005-19, *supra* note 223, at 12, 17 (encompassing Articles 3.3 and 6.10).

information covered by this exclusion of public dissemination, the topics might include information regarding the structure of a partnership or joint venture submitting a proposal, details of similar projects performed by the proposer, and estimates of the "up-front and on-going capital and operating costs to design, build and manage" the system.[225] Therefore, the public at large may be denied significant information by which to consider and offer comments to the city about its potential vendor selection.[226]

These two examples illustrate the impact that restrictive trade secret law has on a public bidding process for the provision of public infrastructure. These cities are forced to recognize the rights of the bidders to broad trade secret protection under the terms of current trade secret definitions that focus exclusively on commercial concerns. While the cities may attempt to modify those definitions by way of discrete contract terms, the fact remains that it is the broad commercial definition of a trade secret that will likely determine the ultimate rights of the public to access information about the infrastructure we may ultimately use to access the Internet.

Moreover, these examples suggest what would happen if private commercial interests, like secrecy, were not an issue. The City of San Francisco has an open government ordinance; the first words of the ordinance declare, "Government's duty is to serve the public, reaching its decisions in full view of the public."[227] However, according to one news report, San Francisco's RFI/C attracted over twenty bids, of which some were "entirely secret," while others were 90% redacted.[228] Additionally, the first TechConnect meeting was reportedly exempt from the city's Open Government Sunshine Ordinance because of the vendors' "commercially sensitive proposals."[229] Were these businesses not protected by law that encourages and supports the submission of secret bids to the city, the meetings and decisions of TechConnect would be subject to far greater public scrutiny. In other words, were the government the provider of this service, there would be no commercial interest—and hence less secret information—to protect.

---

225. *Id.* at 11-12 (encompassing Articles 3.2 and 3.3).

226. As of this writing, EarthLink and Google have entered into contract negotiations with San Francisco. Press Release, City of S.F., San Francisco Concludes Evaluation of Proposals to Create Universal, Affordable Wireless Broadband Network (Apr. 5, 2006), *available at* http://www.sfgov.org/site/tech_connect_page.asp?id=38562.

227. S.F., CAL. MUNICIPAL CODE § 67.1(a) (2006).

228. Andrew Orlowski, *San Francisco Shows World How Not to Do Muni Wi-Fi*, THE REGISTER, Dec. 23, 2005, http://www.theregister.co.uk/2005/12/23/sf_muni_wifi/print.html.

229. *Id.* "[P]ublic versions" of the responses to the RFP are now available. *See* San Francisco TechConnect, RFP Responses, http://www.sfgov.org/site/tech_connect_index.asp?id=36612 (last visited Oct. 16, 2006) (providing public version of six responses to the RFP). While some are lengthy, how these responses differ from those privately submitted to TechConnect is, of course, impossible to determine, because there is no way for the public to examine those documents.

The problems with this condition are significant and varied. Can and will the public's communications be monitored? Can people rely upon the system to communicate time or substantively sensitive information? Will the system truly serve the disadvantaged; i.e., those who would not otherwise have Internet access?[230] These and many other questions might be unanswerable, or if answered, impossible to verify, given the broad protections of trade secrecy law.

Moreover, as in Cisco's situation, efforts to improve upon these networks, based upon the proposed plans, fall entirely to the provider. Absent such broad protections, others might be able to independently fix problems and create improvements, without having to resort first to fighting for access to information. In sum, while these cities should be commended for identifying the possibility that they may need access to information otherwise protected by trade secrecy, the fact remains that they cannot unilaterally change a state law that is designed not for the protection of the public's interest in access to information, but to ensure the business's interest in keeping information secret.

VI. POTENTIAL SOLUTIONS

As has been shown, it is in the area of public infrastructure that trade secrecy problems become especially pernicious. Precisely because public infrastructure relies heavily on human activity, and man-made principles of behavior and conduct for its governing norms, rules, and laws, we have a greater chance of affecting real and needed change. These rules are not immutable. Our expectations of these entities change over time; we are not bound primarily by what is beyond our reach or grasp, as we are with non-man-made resources. Indeed, our expectations of transparency and accountability can only apply directly to those infrastructure goods and services provided for public consumption by humans.

Thus, in the final part of this Article, I briefly consider how we can assure public access to public infrastructure information, beyond access for the government only.[231] The first focus is on patent law. The basic solution

230. In an April 2006 letter, the ACLU of Northern California, the Electronic Frontier Foundation, and the Electronic Privacy Information Center noted several privacy concerns associated with the operation of municipal WiFi by private entities. Letter from ACLU of N. Cal., Elec. Frontier Found., & Elec. Privacy Info. Ctr., to Chris A. Vein, Acting Executive Dir., S.F. Dep't of Telecomm. & Info. Servs. (Apr. 19, 2006), *available at* http://www.sfgov.org/site/uploadedfiles/dtis/tech_connect/googleltr41906.pdf. The writers urged Vein to negotiate "reasonable privacy rights for users of this network," including assuring that personal information is not shared absent the voluntary consent of the owners and is protected. *See id.*

231. Because I am more concerned about unfettered public access to this information, rather than mere access for governmental agencies or third-party ombudsmen, solutions such as the establishment of a rule requiring that such information be placed in escrow with a government agency are inadequate. Indeed, as discussed previously, once we enter into an escrow system, we

is to abandon trade secrecy altogether and simply require commercial public infrastructure providers to find their protection in patent.[232]

At least from a theoretical standpoint, the idea of patents as the primary substitute for trade secrecy has appeal. Patent law is an arguably more democratic notion than trade secrecy in the context of private provision of public infrastructure, because of its public disclosure requirements and limited duration of monopoly. A patent application, which becomes public eighteen months after filing, must "describe, enable, and set forth the best mode of carrying out the invention,"[233] thus affecting substantial public disclosure to anyone who wishes to understand the operations of the invention.[234] Patent law would also allow a company to capture the full

put power in the hands of entities that might have interests aligned with business. *See supra* note 211 and accompanying text. Even if not aligned to that extreme, such entities would be governed by many interests, including political ones, in deciding who could see what information, and for how long. While such a system might protect trade secrecy concerns for businesses, it runs the risk of merely moving the locus of the problem from private industry to third-party entities keeping business secrets. Of course, it would be helpful if government agencies, when faced with assertions of trade secrecy that aim to limit public dissemination of information, scrutinize and challenge such assertions to assure that they are meritorious. While perhaps an especially time- and resource-intensive undertaking for governmental agencies, such an undertaking would help rein in the improper assertion of trade secrecy over what might otherwise be publicly accessible information.

232. Copyright could also be considered, but patent is the best and most complete substitute.

233. Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., 535 U.S. 722, 736 (2002) (citing 35 U.S.C. § 112 (2000)).

234. One major argument against eliminating trade secrecy protection is that it would discourage private entities from entering the market. *See infra* note 240 and accompanying text. While this critique might have some validity, it is not necessarily true that a company would not engage in public infrastructure projects; rather, they may simply charge more for the good or service, the government may have to buy all rights to the goods and services from the provider, or both. *See* Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 919 (2006) (noting that "efforts to extend the burdens of public law procedural and disclosure requirements to private entities inevitably reduce the economic and administrative advantages that originally led government agencies to privatize or contract out previously public services"). The notion that the existence of trade secrecy may encourage more competitive bids, which might lead to cheaper, better services, highlights the basic concern that transparency may require some economic sacrifices. To address such concerns, Professor Frischmann notes that absent market-based incentives, private infrastructure providers could be rewarded by the following: (a) direct government subsidization, (b) tax incentives, (c) cooperative research plans, and (d) encouraging joint ventures. Frischmann, *supra* note 18, at 136. While beyond the scope of this Article, an examination of these solutions, combined with an analysis of (a) the relevant markets for a given good or service, like the limited market for a voting machine versus the larger market for Wi-Fi technology, and (b) the potential ability of a technology to be utilized in contexts that are both commercial and public, would be helpful to address the potential economic impact of eliminating trade secrecy in favor of patent protection. Additionally, one may be concerned that under such a system, the public would receive a "second best" version of the product or service; the private sector getting the best product with the newest technology because trade secrecy is in place. While a reasonable concern, even if it happened, market forces would likely prevent such an occurrence for a long period of time. Presumably, if the acquired product was substandard, there would be interest in finding a better version. Thus, should a substandard product be acquired, a business's

economic value of the company's patented efforts for a significant time, thereby preventing any argument of a takings problem.[235]

In contrast, while it allows reverse engineering and independent discovery (often a time intensive or impossible endeavor, or both), trade secrecy by its very definition abhors both transparency and public accountability. Therefore, abandoning trade secrecy for private entities engaged in public infrastructure and limiting protection to that which is patentable is likely the right, if not perfect, answer.[236] Whether this would take the practical form of an additional "public infrastructure" element in the definition of a trade secret or an affirmative defense to an action alleging misappropriation is less significant than the notion that there is a theoretical disconnect and that patent law may be a ready-made salve to much of the sting of the loss of trade secrecy for public infrastructure projects. Indeed, even where there is a limited market for the specialized device, like Diebold's voting machines, patentability would still allow the inventor to sell the product to its customers and license the product to its competitors. Whether this is the most efficient way to provide public infrastructure is, for purposes of this Article, secondary to the fact that

---

interest in serving that market might encourage a rival to compete and provide a better product.

235. A concern might be raised that by eliminating trade secrecy protection for private entities engaged in public infrastructure altogether, the effect constitutes a taking by the government under the Fifth Amendment. The Supreme Court has recognized that extinguishing a property interest, including a trade secret, may constitute a taking. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1003 (1984). Generally, subject to certain conditions, so long as there is a "regulatory scheme with both burdens and benefits," a give-and-take exchange will not be considered a taking. Phillip Morris Inc. v. Reilly, 113 F. Supp. 2d 129, 144 (D. Mass. 2000). The argument against a takings claim is that the voluntary submission of non-patentable trade secret information in return for the pecuniary advantages of providing public infrastructure without government competition—a give-and-take—is not a taking. *See* Megan E. Gorman, Note, *Going Up In Smoke: The Effect of* Phillip Morris, Inc. v. Harshbarger & Phillip Morris, Inc. v. Reilly *on the Takings of Intellectual Property*, 33 RUTGERS L.J. 771, 796-98 (2002) (approving, in the context of the Massachusetts government's requirement that tobacco companies reveal the ingredients of cigarettes and smokeless tobacco, the First Circuit Court of Appeals' analysis of a takings challenge that "the voluntary submission in exchange for advantages of a registration [to do business in Massachusetts] could 'hardly be called a taking'" (quoting Phillip Morris, Inc. v. Reilly, 2001 WL 1215365, at *10 (1st Cir. Oct. 16, 2001))). Moreover, the continued existence of patent protection would militate against the argument that public infrastructure providers have lost all protection of their trade secrecy rights.

236. It is important to recognize that businesses face real alternatives to secrecy. *See* HENRY CHESBROUGH, OPEN INNOVATION 170-74 (2003) (discussing Intel's practice of publishing, rather than patenting, those inventions that they would "prefer to put into the public domain," in an effort to benefit their business); Jim Chen, *Biodiversity and Biotechnology: A Misunderstood Relation*, 2005 MICH. ST. L. REV. 51, 79-81 (2005) (discussing the public benefits of patent law over trade secrets and noting that trade secret law "by design, keeps information concealed [and] [b]y contrast, patent [law is] designed to deliver privately held information into public hands"). *But see* Dan L. Burk & Mark A. Lemley, *Is Patent Law Technology-Specific?*, 17 BERKELEY TECH. L.J. 1155, 1161-63 (2002) (noting that § 112 of the Patent Act imposes minimal disclosure requirements for software).

transparency and accountability are increased under such a system.[237]

By this solution I am not suggesting that patents are purely democratic, that all patent applications are thorough and complete, or that patent constitutes the perfect substitute.[238] Clearly, there are certain ideas and processes that are better suited to trade secrecy protection.[239] However, the fact remains that trade secrecy law serves interests that are anathema to basic public values, and the sacrifice to greater public accountability must, by definition, diminish some of these tangential advantages.[240]

This somewhat drastic measure is made more appealing because courts have had a difficult time determining what a "public concern" is for purposes of First Amendment protection of disclosure of trade secrets by the press. Professor Volokh has persuasively argued that courts have consistently run into problems when considering situations where the news media is sued for publishing a trade secret leaked to it by someone in violation of their duty of confidentiality, but without encouragement from the news media.[241] Therefore, a possible solution of relying on the courts to simply allow dissemination of trade secrets deemed a "public concern" would likely continue to run into the same subjective judicial problems regarding where the line between a "public concern" justifying disclosure and a "private concern" prohibiting disclosure should be drawn.[242]

---

237. Alternative solutions may be to retain trade secrecy in the research and development stage only, where it has enormous potential value to a commercial entity, or to limit the amount of time that trade secrecy protection may be applied to public infrastructure trade secrets. Such solutions would address some of the problems that industry would face if trade secrecy were eliminated in its entirety for public infrastructure projects.

238. Patent law has been subject to much criticism in recent years, for reasons ranging from the overuse of patents in the computer software context to the amount of information that is actually revealed in a patent application, and is therefore not the perfect solution. I acknowledge that there may be items that can only be protected by trade secrecy, and that patent and trade secrecy are not perfect substitutes. But, I submit, the majority of information about which the public would be concerned could be subject to patent.

239. *See supra* note 11 and accompanying text.

240. It should be noted that one criticism of this solution is that particular technologies used in public infrastructure, like code in Cisco's routers, might also be used in normal private commercial markets. In that case, a provider would face a choice: forgo trade secrecy, patent the invention, and sell it to the public and governments; or keep the trade secrets (thereby challenging competitors) and forgo the public infrastructure market. While a supplier may choose the latter option in some cases, it is reasonable to assume that other entities will fill the void. In any case, transparency would be achieved. While beyond the scope of this Article, an examination of the substitutability of trade secrecy and accountability in this limited scenario, and more generally in the research and development stage, should be considered.

241. Volokh, *supra* note 60, at 739-42; *see also* Alex Eaton-Salners, Note, DVD Copy Control Association v. Bunner: *Freedom of Speech and Trade Secrets*, 19 BERKELEY TECH. L.J. 269, 282-83 (2004) (criticizing the decision of the California Supreme Court because its "formulation and application of the public concern doctrine was incorrect").

242. Of course, by way of analogy, the United States Supreme Court has struggled with the definition of a matter of "public concern" in First Amendment jurisprudence. *See* Dun &

Additionally, it is worth noting that trade secrecy doctrine is not needed as a vehicle to protect sensitive or potentially dangerous information from falling into the hands of people or entities who may seek to do harm to the United States' public infrastructure. For example, the Critical Infrastructure Information Act (CIIA),[243] passed as part of the Homeland Security Act of 2002,[244] regulates "the use and disclosure of information submitted to the Department of Homeland Security (DHS) [by businesses] about vulnerabilities and threats to critical infrastructure."[245] While the CIIA has been criticized for being superfluous[246] and having an overly broad definition of "critical infrastructure information" that will allow an enormous amount of information to be protected from disclosure to the public,[247] the existence of the CIIA shows that trade secrecy doctrine is not needed to protect sensitive information regarding our public infrastructure from being accessed by those who could use that information to do harm.[248]

Short of abandoning trade secrecy altogether, there are other potential partial solutions. As discussed earlier, the commercial definition of a trade secret could be narrowed, as in the FOIA trade secret exemption,[249] to only apply to information that is actually used in commerce or where its

---

Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 751-52, 758-59 (1985) (applying the "public concern" test to a private plaintiff who alleged defamation based upon the defendant sending an errant credit report to five subscribers and noting that "speech on public issues" is of primary concern to the First Amendment). For example, it seems reasonable to assume that the operation of a voting machine and its impact on one's ability to cast a recorded vote would have to qualify as a "public concern" under First Amendment analysis.

243. 6 U.S.C.A. §§ 131-134 (West 2006).

244. Pub. L. No. 107-296, 116 Stat. 2135 (2002).

245. GINA MARIE STEVENS, HOMELAND SECURITY ACT OF 2002: CRITICAL INFRASTRUCTURE INFORMATION ACT, Summary (2003).

246. *See* Brett Stohs, *Protecting the Homeland by Exemption: Why the Critical Infrastructure Information Act of 2002 Will Degrade the Freedom of Information Act*, 2002 DUKE L. & TECH. REV. 18, 20 ("[T]he private sector exemptions are redundant and unnecessary. [FOIA] contains several exemptions that protect information given to the government by private entities.").

247. *See id.* at 23 (quoting Representative Jan Schakowsky as saying that this definition is a "loophole big enough to drive any corporation and its secrets through"); Editorial, *Overkill in the Name of Security*, ST. PETERSBURG TIMES, July 14, 2002, at 2D, *available at* http://www.sptimes.com/2002/07/14/news_pf/Perspective/Overkill_in_the_name_.shtml (criticizing the legislation as providing an incentive for companies "to share all sorts of irrelevant information with the government" because it would then be protected from public disclosure); Beryl A. Howell, Op-Ed., *Information Overload*, LEGAL TIMES, June 2, 2003, at 52 (suggesting that DHS will become a "dumping ground for large amounts of irrelevant and improperly marked business information").

248. It is beyond the scope of this Article to analyze whether the CIIA is a proper method to protect trade secret information. Nonetheless, the existence of this law suggests that one could craft an exemption under FOIA that protects certain public infrastructure trade secrets from disclosure, and thereby dispense with using the commercial definition for such purposes.

249. *See supra* note 154 and accompanying text.

disclosure would pose an immediate threat to the security of the infrastructure itself. In this way, the information that would be protected from disclosure would be less than that covered by the current all-encompassing definition, and would reflect more respect for the legitimate needs of the public.

Alternatively, the duration of trade secret protection could be limited. For example, a public infrastructure trade secret could be protected for up to five years, at which time the holder of the secret would be required to submit the trade secret to a government agency to hold in escrow. Either or both of these solutions in tandem would address the most pernicious aspects of trade secret protection of public infrastructure—namely, the overly broad definition and potentially unlimited duration of a trade secret—without wholesale abandonment of the doctrine.[250]

A final partial solution is to change the remedies allowed under a trade secret claim by denying injunctive relief for the misappropriation or innocent release of public infrastructure trade secrets and limiting relief to monetary damages. This change would be nearly as drastic as denying trade secret protection altogether, as injunctive relief is the most sought after, and most important, remedy in trade secret misappropriation cases.

The typical trade secret injunction, which prevents the further dissemination or use of the subject trade secret, attempts to put the "genie back in the bottle."[251] The effect is to put a lid on further examination of the trade secret—again, against a core value of public governance. While this does not prevent the public harm of keeping such knowledge secret from a deserving public, it would at least prevent the quashing of public examination once begun. Therefore, consideration of limiting relief to monetary damages when public infrastructure trade secrets are misappropriated should be explored. Such damages would be paid by the misappropriating competitor, and could include the complete disgorgement of profits earned by the misappropriating entity, but the public benefit of disclosure would remain. The public knowledge gained, and, by dint of the public disclosure of the secret, the possible improvements thereon, would not be denied.

To be sure, none of the proposed solutions, save abandoning trade secrecy altogether in the context of public infrastructure projects, are fully satisfactory, as they do not fully harmonize the differing theoretical underpinnings between these competing doctrines. The proper goal is to have public transparency without coercion, absent the

250. Of course, any alteration of the contours of trade secret protection would have to pass constitutional muster by not "frustrat[ing] the achievement of the congressional objectives served by the patent law." Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 154-56 (1989) (reaffirming Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 484, 489-90 (1974), and its analysis of why the subject trade secret law did not conflict with Congress's patent objectives and goals).

251. *See supra* notes 194-95 and accompanying text (discussing the Cisco settlement).

regulatory/administrative process or resort to the courts. None of these options, save complete elimination of the law in the area of public infrastructure, reset the system to a default of transparency; rather, they force some modicum of disclosure where it would not normally exist. The goal is transparency by default, and the absence of complete solutions short of entirely eliminating trade secrecy in this area is perhaps the best argument for why trade secrecy is simply an irreconcilable theoretical mismatch with the values and goals inherent in the provision of public infrastructure.

VII. CONCLUSION

The United States faces an increasing dilemma as it outsources and privatizes infrastructural projects that were once primarily in the purview of government, such as the operation of roads, and witnesses the wholesale development of new forms of public infrastructure that require relatively little from government, such as the Internet. Absent a commitment to public values, private providers of public infrastructure risk alienating the public—their consumers. While abandoning trade secrecy would have some downsides, like forcing businesses to find other avenues of protection for their business interests, absent change we face the real likelihood of finding more and more information regarding our public infrastructure hidden from public view and inspection. The values of commerce will eliminate public values like transparency and accountability from our voting machines, Internet routers, and telecommunications systems.

To address these concerns, trade secrecy must be severely curtailed, if not entirely eliminated, from the world of public infrastructure. Unless we reconsider how trade secrecy is impacting our access to knowledge, increasing amounts of information regarding our public infrastructure will be hidden from public view, the commercial concerns of trade secrecy as applied to otherwise publicly-oriented activities will continue to eclipse the values of transparency and accountability, and a greater number of people will pose Cato's ultimate question to Cisco, Diebold, and all other public infrastructure providers: Are you seeking to instruct or deceive? For everyone's benefit, and despite the potential economic downside, abandoning trade secrecy in this context is the best way to answer that question.