Tailoring Trade Secrecy:

The Moral Imperative of Industry-Specific Application of Doctrine

David S. Levine and Frank A. Pasquale III

Draft—Please do not circulate or quote without permission.

Companies and governments use data to categorize, rank, and rate individuals. Are you a terrorist threat? A good credit risk? A diligent worker or student? Software programs crunch the numbers, delivering silent judgments. A bad credit score may cost a borrower hundreds of thousands of dollars, but it is not clear how it is calculated. The formula is a trade secret, immune from scrutiny. Recommendation engines at Amazon and YouTube affect an automated familiarity, gently suggesting offerings that you may like. But their methods of selection are secretive, driven by economic, political, and cultural agendas that are hard to unravel. So too can Internet access providers ("IAPs") use secret methods to decide what sites to prioritize, and which to block or slow down. Finance companies shroud deals in impenetrable complexity. When the resulting lack of trust pushed the banking system to the brink of collapse in 2008, the Federal Reserve chose to classify its stabilizing interventions as secret, too.

Even familiar technology is far from transparent to ordinary users. To access usable information, those that are interested can hire experts (or look to intermediaries like Consumer Reports) to try to figure out what is going on in their toaster or car. But when it comes to secret sorting mechanisms, it is not even possible to assess the assumptions and values built into the algorithms. This is a dark side of the "big data" movement that few of its supporters want to acknowledge, and even haunts computational sciences, as Victoria Stodden has demonstrated.

Secret methods are also deeply affecting the natural world, in ways that we are only beginning to understand. The energy sector has asserted proprietary information protections for both its drilling methods and its cleanup processes (and chemicals) when spills happen. Because the effects of today's activities can often only be measured and felt months, years and even decades later, the impact of today's secrecy can have ramifications long after the entities that caused the harms dissolve, effectively leaving no one accountable.

What is leading to such a bizarre array of infringements on the public right to know basic features of its finance, energy, and communications systems? We believe that the problem may lie in an improper treatment of trade secrets as a form of intellectual *property* subject to few, if any, exceptions. When abstract methods and processes are treated as property under the patent system, there are limits built into several aspects of the relevant

statute and case law. The term of protection is limited in time and scope. Even in copyright, distinctions between the protection of ideas and facts versus expressions and fair uses allows for lines to be drawn between that which should be propertized and owned and that which should be free from such impediments to its use by all. But when the same are trade secrets, they can last indefinitely, and they are almost impossible to limit. Reverse engineering and independent discovery simply do not work as effective limits when the public interest scope and nature of the information is irrelevant to the analysis. The cost of excess trade secrecy is now a persistent theme in intellectual property scholarship.

This article explores two solutions to the overprotection of trade secrecy. First, within the property paradigm, courts should apply some classic limits familiar from other areas of IP. For example, given the extremely long term of copyright, judges developed a body of fair use case law. When the public interest is at stake, they could demand that certain secrets be subject to limited use by the relevant authorities and/or have a limited duration. Moreover, the classic quid pro quo in patent law, even if watered down in the America Invents Act, between disclosure and monopoly allows for innovators to develop new, better and more innovative goods and services even while the patent monopoly remains intact. Similarly, we could broaden the definition of "value" in trade secrecy to include not just the value of the competitor, but also the value to the public.

However, none of the above solutions squarely address the theoretical morass that underscores trade secrecy. Articulating a unified theory of trade secrecy has been a Quixotic endeavor of several scholars in recent years, and their efforts, while laudable, have (even by their own admission) been not fully satisfactory. While the reasons range from the differing meanings of "improper means" under the Uniform Trade Secrets Act to the range of meanings attendant to labeling information as "property," this Article proposes that the theoretical problem lies in overlooking *how* information is used by the recipient of the information.

Indeed, identifying the intended and actual use of the information by the recipient – the actual misappropriation – is a usually overlooked and/or assumed aspect of trade secret law analysis. And yet, when we identify the use, the theoretical lines become easier to draw and normatively sound because a new use of trade secrets has emerged in recent years. Today, as this Article discusses, the substantive range of trade secrets – from chemical formulas to credit scores -- means that an increasingly important use of a trade secret is not competitive advantage, but for the good of the public at large (i.e., public health or consumer protection). That latter use is anathema to any traditional and prevailing notion of why one may want access to another's trade secret. Indeed, scholars like Stephen Carter in the 1990s may have considered it marginal, if at all. Twenty years and an Internet later, the time to consider this use has come.

Thus, another (and preferred) set of solutions operates within the realm of tort law. Scholars and practitioners have long debated whether trade secret protections are best thought of as forms of intellectual property, or as the natural result of tort law's penalties for unauthorized disclosure of confidential information. The waning of the law of privacy and confidentiality (and unpredictable effect of First Amendment law on it) have probably provoked scholars like Mark Lemley to point up the virtues of treating trade secrets as a form of intellectual property. This approach may increase the certainty of entities that invest in trade secret protected innovation, and may be adequate in a majority of traditional trade secret scenarios like the paradigmatic departing employee or failed commercial negotiation.

But if trade secrecy law cannot achieve the same flexibilities that copyright and patent law doctrine have developed over the years, the cost of an IP-based approach may be too high in the emerging area of what we call "public interest trade secrets". To the extent that flexibility has existed in trade secrecy, it is not by design, but rather borne of the confusion around what trade secret law is supposed to achieve in the first instance. The result has been a malleable doctrine limited usually only by the perspective of the judge. Therefore, we may, instead, need to adopt (or re-adopt) a tort or unfair competition law approach, which can be tailored to individual situations incrementally (via common law adjudication) rather than specified ex ante in statutes like the state laws based on the UTSA.

The courts can achieve that industry- (and use-) specific tailoring along two dominant fault lines in trade secrecy: the relationship between the trade secret holder and its acquirer, and the ownership interest in the information. As developed more fully in this Article, the property conception of trade secrecy works well in the traditional trade secret scenarios where the accessed trade secret is used for competitive advantage by a former employee or business partner. In those scenarios, the relationship between the parties is strong and value proposition is front and center, as the value may be wholly or partially usurped by the alleged misappropriator. Moreover, whether property is defined as ownership or a bundle of rights, focusing on the potentially diminished value of the trade secret through its use by the acquirer allows for the balancing that scholars like Tait Graves, Mark Lemley and Michael Risch have extolled.

But when dealing with nontraditional scenarios like those discussed in this Article, the property theory asks the wrong questions. Where the relationship between the parties is weak and more attenuated and the use by the acquirer is for reasons other than usurpation of value by commercial competition, the property conception tends to overprotect the alleged trade secret and ignores the reason for and use of the acquired trade secret. Thus, the better question to ask in those scenarios is not the impact on property conceived by the impact on value, but rather whether there is a misappropriation by the acquirer through

access to the information and its eventual use. The right questions for this scenario are asked, and to the extent that commercial morality is offended in the process, the courts have a theoretically sound basis to deny access. This theory and framework fits within IP law "solutions" to overpropertization. Scholars are increasingly inclined to frame the issue as an operationalization of the insights of Michael Carroll's "Uniformity Costs" concept: how to shape doctrine so that it respects the unique economic conditions (and moral imperatives) related to specific industries. One way to do so is to insist on the autonomy of a subject matter defined legal field (versus the trans-substantive aspirations of, say, contract, property, or intellectual property law). Frank Easterbrook's classic "law of the horse" critique has assailed that autonomy by warning about the distortionary effects of applying different laws to different sectors. But that anxiety seems to have faded in at least a few domains, such as finance, energy, media, and ranking and rating systems. In each of these areas, a long history of regulatory actions has already established a distinctive law.

We predict that, in coming years, there will be a growing conflict between the needs of regulators and/or public ombudsmen for information in the fields of finance, energy, and media, and the business strategies of firms that want to keep their methods secretive. So far, and with very few exceptions, business has won a series of notable victories over the public right to know, and has even deflected dedicated, confidential internal review bodies (like the Office of Financial Research in Treasury) from obtaining critical data. As such cases are litigated in the future, judges need to take care to either build flexibilities into trade secrecy law as an intellectual property doctrine, or to treat disclosures as merely *potential* torts, which must be judged as such based on the totality of the circumstances, including the relationship between the partiesand the likelihood of harm flowing from the use of the trade secret by the acquirer.

The argument proceeds as follows. Parts II to V describes current controversies over access to proprietary information in energy, media, and finance settings. Part VI lays out the doctrinal foundation of trade secrecy law, emphasizing its roots in both tort and IP law. Part VII suggests how trade secrecy law can be tailored to the unique challenges of information access in each industry, with either IP or tort-based interpretations of current statutes and case law. Part VIII concludes by situating the argument in a larger context, explaining the normative concerns that need to be balanced in the emerging laws of energy, finance, and media information.

Legal doctrine (and scholarship) gain quasi-scientific authority and rhetorical force by encouraging specialization. There are contract, tort, and property law experts; the metaphors of property have in turn bred specialties like real estate and intellectual property law; and subspecialties flourish within intellectual property law (including patent, trademark, copyright, and trade secret law). Some scholars spend most of their career within a sub-sub-specialty, like fair use in copyright law, or patent remedies.

Specialization can help "work the law pure" in given fields, making it easier to classify disputes and harmonize precedent. But it threatens to distort the scholarly endeavor when it fails to take into account the full range of policy concerns raised in a given field. This article examines some untoward consequences of specialized trade secret doctrine.

In our past work, we have isolated instances where trade secrecy poses a threat to public values. For example, Levine* … Pasquale's chapter in *The Handbook of Research in Trade Secrecy* focused on trade secret protected ranking systems. Often, the outputs of these ranking systems are completely protected by the First Amendment, and trade secrecy is deployed to keep both market and governmental actors from understanding exactly how data inputs are being processed (or, even more troublingly, what data is even being input into these systems).

Unfortunately, neither doctrine nor (except for a few notable exceptions) scholarship has properly recognized our concerns. Just as patent law refuses to consider the "moral utility" of inventions and leaves regulatory functions to agencies like the FDA or SEC, trade secrecy law has remained largely agnostic as to the potential ill-effects of the secrecy it protects.

We use this paper to make two points. First, the theoretical and practical problems we have pointed out in past work on infrastructure and ranking systems are not isolated to those corners of the economy. Rather, they afflict the financial, medical, and consumer reputation sectors, and threaten to make those critical parts of our economy effectively ungovernable. Second, trade secrecy never operates in isolation. Rather, it is part of a coordinated and well-planned business strategy to gain information advantage over competitors and consumers and to avoid monitoring and regulation. Trade secrecy, on its own, may seem like an innocuous way of assuring innovators low-cost protection for their work. But when combined with exemptions to FOIA laws, attorney-client privilege claims, homeland security laws on critical infrastructure, overwhelmed regulators, increasingly high pleading standards, and technical complexity, they can act as a "Ring of Gyges," ending the very possibility of accountability for destructive actions.[1] Apart, each tool to keep information confidential is limited. Together, state secrets, trade secrets, and the other protections create an impenetrable wall of secrecy.

Given the multiple other methods of assuring business confidences, it is well past time to tailor trade secrecy theory and practice to the public values it is supposed to serve, rather than permitting its indiscriminate application to continue to undermine the very possibility of market discipline and legal responsibility in critical sectors of the economy.

[1] All of the other strategies of secrecy have (at least in principle) regulatory limits, but trade secrecy has, in a few leading cases, been protected as property under the 5th Amendment.* OR: **Critical mass of secrecy**