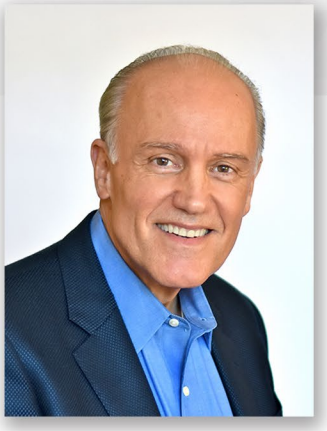

JAMES POOLEY

International Trade Secret Expert

pooley.com

ADDRESSING THE "REASONABLE EFFORTS" REQUIREMENT THROUGH EXPERT TESTIMONY

James Pooley

Introduction

The Uniform Trade Secrets Act requires that a trade secret be subject to "reasonable efforts under the circumstances to maintain its secrecy."[1] The Defend Trade Secrets Act similarly requires that the owner have taken "reasonable measures to keep such information secret."[2] But what is reasonable and what isn't? And how do you prove one proposition or the other? We will examine here the role of the expert in assisting the trier of fact to reach a conclusion.

Rule 702 of the Federal Rules of Evidence permits a court to accept expert testimony when the proponent has demonstrate each of four requirements: (a) the expert's specialized knowledge will "help the trier of fact" determine an issue; (b) the testimony is based on sufficient facts; (c) the opinion is grounded on "reliable principles and methods" which (d) have been "reliably applied" to the facts of the case.

Use of experts is common in trade secret litigation. Where the subject matter of the claimed secrets is highly technical, retained specialists will be presented by each side to help explain the evidence in a way that the judge or jury can understand its nature and whether it is likely to have been misappropriated by the defendant. And in almost every case, damage experts will be called to provide an opinion of the amount that should be paid by the defendant in case misappropriation is found.

But despite the universal requirement that a plaintiff prove "reasonable efforts," there have been only a few opinions reporting on how that element is established or disproved through experts.[3] Instead, most of the case law seems to come from attempts to test the issue by summary judgment, the majority of which fail because the courts see it as a fact issue for the jury.

---

[1] Uniform Trade Secrets Act § 1(4).

2 18 U.S.C. § 1839(3)(A).

[3] See, e.g., United States Gypsum Company v. LaFarge North America Inc., 670 F. Supp.2d 768, 773 (N.D. Ill. 2009) (approving a forensics expert's testimony on the reasonableness of computer security measures); Proofpoint, Inc. v. Vade Secure, Inc., 2021 U.S. Dist. LEXIS 118313 at *2-*4 (N.D. Cal. June 24, 2021) (denying challenge to testimony of the author on grounds of offering legal opinion); Neural Magic, Inc. v. Meta Platforms, Inc, 659 F.Supp.3d 138, 172-174 (D. Mass. 2023) (denying motion to strike opinion of law professor because she did not have expertise in the technology of some protective measures; and FMC Techs. v. Murphy, 679 S.W.3d 788, 801-805, 808-812 (Texas App. 1st Dist. 2023) (expert qualification did not require specific industry experience, and risk management methodology was reliable and related to the plaintiff's focus on patents instead of trade secret protection).

Based on my experience and review of reported cases, the "reasonable efforts" issue appears not to have been seriously challenged in most disputes. In part this may be the result of a sensible assessment in those cases that the facts do not suggest that the plaintiff was sufficiently careless. Alternatively, the defendant's misappropriation may have been so obvious that asserting lack of reasonable efforts might be seen as insulting to the jury's sense of morality.

The Contextual Nature of Reasonableness

But where the plaintiff appears to have been less than rigorous in its efforts to maintain control over its secrets, the issue may be put into play. The question then becomes how to address it. Keep in mind that traditionally (that is, under the common law and the First Restatement of Torts), "reasonable efforts" was only a factor to be considered, not a required element. It was only with the UTSA and the reformulation of the common law under the Restatement (Third) of Unfair Competition that reasonable efforts became an element of a trade secret claim. Even so, in the early going courts were generally quite forgiving of any failures by the plaintiff, tending to reject challenges where there had been any sort of attention paid to security, such as use of basic confidentiality agreements. More recently, with additional jurisprudence focused on the issue, summary judgment for the defendant on this basis has become more common.

As already noted, there is not a great deal of useful teaching that can be extracted from the reported cases, given that most are decided on summary judgment. And of course because the measure is reasonableness "*under the circumstances*,"[4] it might seem difficult to apply a consistent methodology to answer the question. However, some generalization is possible. For example, while a large, hierarchical company would be expected to have well-developed policies and procedures, with specific access controls and formal training programs covering the handling of confidential information, less formality typically is required of a small business where the employees know each other well and share multiple responsibilities.[5]

The reason that we can make that distinction is that "reasonableness" is highly contextual, and in the case of the small business there is inherently less risk of misunderstanding what it means to keep everything confidential. Indeed, the touchstone of the reasonableness inquiry is a classical risk analysis framework, in which threats to confidentiality are measured against the costs of reducing the risk and the value of the information to be protected. As one court put it, the law requires "an assessment of the size and nature of [the] business, the cost to it of additional measures, and the degree to which such measures would decrease the risk of disclosure. What may be reasonable measures in one context may not necessarily be so in another."[6] As expressed in the Restatement (Third) of Unfair Competition, risk is determined by the "foreseeability" of misappropriation, and this is weighed against "the availability and cost of effective precautions" against it, "evaluated in light of the economic value of the trade secret."[7]

---

[4] It is fair to assume that "under the circumstances" is inherent in the "reasonable measures" standard of the DTSA, since what is "reasonable" necessarily depends on context.

[5] See Northern Electric Co. v. Torma, 819 N.E.2d 417, 428 (Ind. App. 2004).

[6] *In the Matter of Innovative Construction Systems, Inc.*, 793 F.2d 875, 884 (7th Cir. 1986).

[7] *Restatement (Third) of Unfair Competition*, § 43, comment c.

A Methodology that Can Assist the Trier of Fact

Given that what is "reasonable" depends on varying circumstances, and because juries cannot be expected to come to court understanding the special risk environment of most businesses and what options are available to address risk, it follows that the trier of fact in these cases would almost always benefit from receiving evidence of those matters. In the abstract then, it should be easy to see the value of providing expert testimony to help inform the jury's determination of reasonable efforts.

To best understand how the plaintiff should have been treating its confidential information, it makes sense to analyze the facts as would a hypothetical management consultant arriving at the company to help guide it through a risk analysis.[8] That process begins with identifying the secrets that matter: what are the company's most important information assets, measured either by their impact on margins or other efficiencies, or by the perceived harm that would be caused by their loss or contamination? This doesn't imply the need for an exhaustive "inventory" or "audit," but typically a high-level, categorical determination of what management thinks are the most important kinds of information. Inherent in this procedure is a rough assessment of the relative value of those assets, so that priorities can be established.

The next step in the risk management process is to identify the "threat environment," that is, to estimate the chance that these assets will be lost or damaged in some way, either through carelessness (by far the more likely source) or because some malicious actor has targeted the company for espionage. This means both identifying the threat as well as determining how likely it is to occur (sometimes measured over a period of time), along with the consequence to the company if it does occur.

Based on an understanding of the value of each category of information and the risks that it faces, it is then possible to consider what ways might exist to reduce or even eliminate the risk, and to allocate resources adequate to support the mitigation. This is where checklists can become useful, as a way to inform management's brainstorming. What policies and procedures have been established? How are the company's facilities secured? What sort of confidentiality training is required of employees? How are NDAs used with employees and third parties, and who manages compliance for both inbound and outbound information? How is access to information in the company's IT systems controlled? How are communications designated? There are almost limitless variations on these practices, and any decisions will be driven by an understanding of their impact as well as their cost, in terms of both money and inconvenience. (All security measures involve some trade-off of convenience; think for example of two-factor identification, which slows a transaction while making it more secure.)

---

[8] A good description of the process can be found in *Protecting Trade Secrets From Cyber and Other Threats* (CREATe.org, 2018), available at https://thesedonaconference.org/sites/default/files/conference_papers/%5B3.1%5D%20CREATe.org_Protecting%20Trade%20Secrets%20from%20Cyber%20and%20Other%20Threats_2018.pdf. See also *The Sedona Conference Commentary on the Governance and Management of Trade Secrets*, available at https://thesedonaconference.org/node/10030.

In the context of designing or improving a company's information protection program, decisions are made about accepting costs based on avoidance of risk. In the context of litigation, where those choices have already been made, a company's decision not to endure the cost of certain security measures might be seen as reflecting its view that the relevant information is not sufficiently important or valuable, or that the risk is low. This relates to the "signaling effect" of efforts taken – or not taken – to protect the company's information assets. In other words, strong security measures generally send a message to employees and outsiders that the enterprise cares deeply, while relatively weak measures can send a different message, indirectly increasing risk.

Of course, not all companies engage in structured risk management regarding their trade secrets, and so in litigation the expert has to reconstruct from the available record (pre-existing documents, deposition testimony) a fair representation of how the company has addressed information security, and how its efforts might compare to an "ideal" approach. That said, the law does not require perfection, and management has a great deal of discretion in how it seeks to protect all the company's assets, including its intellectual property. The "reasonable efforts" requirement exists to ensure that plaintiffs have engaged in a certain amount of self-help before requesting intervention by the courts. What is "reasonable" therefore should be determined according to the specific circumstances faced by the plaintiff in its business. To the extent that its efforts reflect the risk-value-cost approach applied to other kinds of assets, the decision of the trier of fact will be fact-based and objective.

Common Errors of Experts

The most common misperception promoted by experts on this subject is that "reasonable efforts" represents a single approach, consisting of some aspirational published standard,[9] or examples gleaned from case opinions where courts have cited with some degree of approval various practices, most commonly the use of NDAs. The problem with approaching the issue this way is that it ignores the essentially contextual nature of the issue. It is efforts "reasonable *under the circumstances*" that matter. To provide an appropriate analysis requires attention to the unique circumstances of the plaintiff's business and the security issues that it faces. Simply put, there is no one-size-fits-all way to answer the question.

A key indicator of this homogenized perspective is reference to a list of security techniques, with a "check the box" approach. For example, the box might be employee training, and because there is some sort of training provided, this aspect is deemed satisfied. In the process the expert may ignore the type of training, its frequency, and whether there is any testing or other follow-up. That is not to say that intense and frequent security training for all employees is necessary for every company to meet the reasonable efforts standard; but for some companies, given the nature of their risk environment and the vulnerability of their secrets, such a program may be seen as indispensable.

The other common category of error relates to the qualification for someone to testify helpfully on this subject. Some assume that a company insider, particularly one with domain expertise in HR or IT, automatically qualifies because he or she is so familiar with all of the security-related activities of

[9] For example, the NIST Cybersecurity Framework, or ISO27001.

the business. But if those activities are not grounded on an analysis of the organization's specific risk environment, the observation of "reasonableness" is not tethered to any methodology and begs the most important underlying questions.

Similarly, it can be dangerous to rely on an expert solely because they possess deep industry knowledge. Although it can be helpful to know what peer companies are doing, a presentation only at that level may fail to take into account the special circumstances of the plaintiff's operations. And the same may be said for someone whose only qualification is as a lawyer, unless they have substantial experience working with companies to help them create or improve their trade secret protection programs, and they are willing to present their analysis as a matter of business risk management, rather than as a matter of summarizing what they see in the reported cases.

Conclusion

Companies that rely on trade secrets — which is to say virtually all enterprises, local and global — should assess their policies and practices directed at managing the risks, just as they do with their other business assets. In particular, when they consider the possibility of litigation they should take a hard look at how their management will be judged under the "reasonable efforts" standard. And defendants in trade secret litigation should look at this element of the plaintiff's case just as skeptically as any other aspect. Here, as with other issues beyond the understanding of the layperson, a well-qualified expert can help the trier of fact appreciate what is and is not "reasonable."

James Pooley is a lawyer focusing on the law and management of trade secrets, as an advocate, advisor and neutral. He has testified often as an expert witness on the issue of reasonable efforts. More information is available at www.pooley.com. This paper was originally prepared for the 2019 Trade Secret Summit of the American Intellectual Property Association and has been updated for the 2021 Summit.