

Book Review Trade Secrets: Law And Practice

General Editors: David W. Quinto and Stuart H. Singer,
Oxford University Press Inc. 2009

By John T. Ramsay, Q. C.

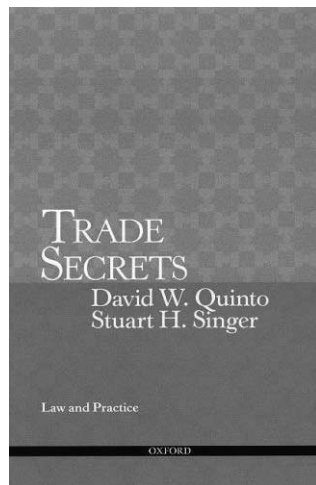
Although the stated emphasis of this book is trade secret litigation, it is an excellent resource for the non-litigation lawyer, as well as individuals charged with managing their company's trade secrets. It is a very readable book with many checklists and sample forms.

The book provides case law support for the principles developed, but it is more focused on the principles than on the intricacies of each of the cases, which makes it much more accessible to the practitioner.

Chapter 1 predictably provides a summary of what is protectable by trade secrecy law in the United States. An illustration of the compact and concise treatment of several topics at once comes at page 5-6:

Unlike the requirement for patentability, information need not be novel to be protectable. In this regard, "the scope of protectable [sic] trade secrets is far broader than the scope of patentable technology." A trade secret may be a device or process that is anticipated in the prior art or that constitutes a mere mechanical improvement. A trade secret may also consist of information known to competitors, provided that it is not "generally known." Although the language of the USTA is worded in terms of general public knowledge, it makes sense to focus upon the knowledge held by competitors in the field. If the principal entity that could obtain economic benefit from the information is aware of it, there is no trade secret.

A trade secret may include elements that are in the public domain if the trade secret itself constitutes a unique, "effective, successful and valuable integra-



tion of the public domain elements." Information may be protectable as a trade secret even if it may be reverse engineered, provided that the reverse engineering cannot be accomplished easily, quickly, or inexpensively. If the information could be reverse engineered easily, it would be "readily ascertainable by proper means" by persons who could obtain economic value from its disclosure or use and, hence, would not qualify as a trade secret.

The issue of "information in the public domain" is correctly reduced to "information not generally known or readily ascertainable." As to "readily ascertainable," they write at page 15:

As suggested above, information is "not readily ascertainable" if it is not economically feasible to obtain. Information will be deemed not readily ascertainable if "the duplication or acquisition of alleged trade secret information requires a substantial investment of time, expense or effort." Regardless of whether others have yet to think of it, information will be deemed "readily ascertainable" if it is "obvious."

When reading this book, I was looking for resources that might provide guidance as to what are the "reasonable security measures" that are necessary to be taken for information to qualify for protection as a trade secret. The authors indicate that any such search for a clear black and white rule may be in vain. They write at page 16:

As with other elements of the test to determine whether information is protectable as a trade secret, the courts take varying approaches to determining whether information has been the subject of "reasonable" efforts to maintain its secrecy. Some place great emphasis on evidence that, for whatever reason, the information has remained unknown to persons who could derive economic benefit from its disclosure or use. Other courts focus on the type of safeguards that were employed to protect the secrecy of the information, placing comparatively little emphasis on whether they were effective. The latter courts seem motivated

by a belief that if the plaintiff has not extended itself to protect its business information, the courts should not be asked to make an effort to do so either. Some courts require that allegations of the steps taken be more than “bare bones” allegations tracking the language of the statute.

There is no bright-line test to determine what amount or types of safeguards are reasonable to protect the secrecy of proprietary information. The Seventh Circuit has said that such a determination “requires an assessment of the size and nature of [the plaintiff’s] 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.” For example, “expectations for ensuring secrecy are different for small companies than for large companies.”

They write at page 17:

The “reasonable efforts” undertaken to maintain secrecy need not be perfect because courts recognize that some mistakes will be made. “[W] here . . . security lapses [a]re not the cause of . . . misappropriation, those lapses should not be the basis for denying protection.” “Heroic” measures need not be employed to protect secrecy.

They provide a long list of safeguards that “have been sufficient to establish reasonableness under the circumstances of the case” [p. 19–21] and [p. 22–3] another list of security measures that have been found to be inadequate (after they caution us that there are “no hard and fast rules for determining what security measures are inadequate”) [p. 22].

Chapter 2 focuses on litigating trade secret actions and provides material not normally found in traditional trade secrecy books. Topics include Alleging Trade Secret Misappropriation, Elements of Misappropriation Claim, Alleging Alternative Claims, Requirement to Identify Trade Secrets with “Reasonable Particularity,” Preliminary Injunctive Relief, Choosing an Expert, Discovery Tactics, Remedies, Settlement and Procedural Considerations.

The authors expressed concern about the effectiveness of protective orders. They write at page 86-7:

Notwithstanding that parties typically enter into protective orders providing that highly confidential information may be designated as “attorneys’ eyes only” to prevent the defendant from learning the plaintiff’s trade secrets, there is a widely held belief among practitioners that such protective orders are susceptible to “leakage.” That can occur even if, as is almost always the case, counsel for

the defendant is both honest and ethical. In trying to prepare an effective defense, counsel may ask his or her client questions based on information obtained pursuant to the protective order with a specificity that allows the defendant to infer what the plaintiff’s secret is. Or, one of the plaintiff’s own attorneys might inadvertently fail to designate highly confidential information as “attorneys’ eyes only,” thereby allowing defense counsel to share it with the defendant. Still further, in-house counsel may be allowed to see and possess “attorneys’ eyes only” materials if their role is simply to advise the defendant with respect to legal questions, as opposed to participating in business decisions, and there is no indication that in-house counsel are disposed to violate the protective order. Regardless of the integrity of in-house counsel, a plaintiff will legitimately worry that if its trade secret information is present at the defendant’s place of business, the wrong eyes may see it. Accordingly, a trade secret misappropriation plaintiff may want, as a tactical matter, to allege misappropriation only of its less valuable and less sensitive secrets.

Chapter 3 focuses on the defendant’s perspective in trade secrecy litigation. I found their comments on reverse engineering of particular interest [p 165-6]:

Reverse engineering is defined as “starting with a known product and working backward to divine the process which aided in its development or manufacture.” In *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, the Supreme Court observed that reverse engineering “may be an essential part of innovation,” potentially “lead[ing] to significant advances in the field.” For this reason, the law provides that “any person who actually acquires the information through an examination of a publicly available product has obtained the information by proper means and is thus not subject to liability.”

A defendant may rely on reverse engineering in either of two ways. First, a defendant may show that it actually learned the plaintiff’s trade secret through reverse engineering and therefore did not acquire the trade secret improperly. Second, a defendant may show that it could have reverse engineered the plaintiff’s product as a means to

■ John T. Ramsay, Q.C.,
Partner, Gowling LaFleur
Henderson, LLP Barristers &
Solicitors, Calgary,
Alberta, Canada
E-mail: john.ramsay@gowlings.com

establish that the plaintiff's secret was "readily ascertainable" and, hence, not entitled to trade secret protection.

If the defendant obtained the plaintiff's secret by reverse engineering a product it obtained lawfully, the defense is established. It is irrelevant what trials and tribulations the defendant may have endured to accomplish its feat. If, however, the process of reverse engineering was significantly expensive or time-consuming, the defendant will have demonstrated that the secret is probably not "readily ascertainable" by others and may thereafter claim the reverse-engineered trade secret as its own.

In contrast, showing that the defendant could have reverse engineered a product or re-created a customer list or database from publicly available sources does not automatically result in litigation success for a defendant. There is no bright-line test to determine when reverse engineering is sufficiently burdensome that a plaintiff's secret may be said to be "not readily ascertainable."

For the non-litigator, Chapter 4 is one of the jewels of this book, "Corporate Trade Secret Protection Plans and Practices," along with Chapter 5, "Hiring and Terminating Employees." These chapters are loaded with checklists and sample forms and requests. An unusual one in Chapter 4 is the "Manufacturing Protection Checklist," as follows:

Manufacturing Protection Checklist

- Do not allow employees without a need to know to visit either the manufacturing area or laboratory areas where manufacturing techniques are perfected;
- Require that any third parties having knowledge of the manufacturing equipment (including equipment manufacturers and maintenance persons) sign nondisclosure agreements;
- If the identity of a particular supplier is important, ask the supplier to ship its products in unmarked containers;
- If the types or grades of the chemicals or minerals used are important, ask that they be mislabelled or, at a minimum, legended; and
- If possible, perform different steps in the manufacturing process at different locations.

Just like Chapter 4, Chapter 5 "Hiring and Terminating Employees" is a highly practical resource. There is an excellent checklist of "Good Hiring Practices," too long to quote here. There is a sample Employee Confidentiality and Invention Assignment Agreement and an Exit Interview Checklist, all of which are very useful.

Chapter 6 focuses on criminal aspects of trade secrecy and misappropriation. The authors write:

A compliance and ethics program should therefore include "standards and procedures to prevent and detect criminal conduct," including "internal controls that are reasonably capable of reducing the likelihood of criminal conduct." Such a plan should be designed for the specific company and the real world risks that it faces, taking into consideration the size of the organization, the extent to which it hires foreign facilities or has foreign affiliates or venture partners, the rate at which it is hiring new employees, the extent to which it is a government contractor, the extent to which it outsources any of its development work, the value of its technology, the aggressiveness of its competitors, and whether the company has had past problems involving trade secret theft and its exposure to third-party trade secrets. Separate but coordinated programs should be established for foreign subsidiaries and larger companies should use their economic influence to persuade vendors and "business partners" to adopt appropriate compliance plans.

A company may not rely on a general policy statement articulating its respect for the intellectual property of others. Instead it must "establish standards and procedures to prevent and detect criminal conduct." Such standards should be sufficiently specific to provide meaningful guidance to all employees in the performance of their jobs. In addition, the plan should set forth a procedure to follow when a problem is discovered, including who should be notified and what sort of investigation should be conducted.

The 90-page Appendix provides an overview of trade secrecy laws of selected states.

This is a very welcome practitioner's guide. It is readable, accessible and practical. A valuable addition to any library. ■