Secrecy and National Commercial Information Policy

HAROLD C. RELYEA

THE OBJECT OF BUSINESS is sales and profits. And businesses go to great lengths to make known or advertise what they have to sell. But they also seek control over information concerning their sales and the production of what they are selling—goods and services. Secrecy, it has been said, is the soul of business. And the penchant for secrecy may be explained in a variety of ways: market advantage, investment protection, quality control, or production security, to name but a few considerations. Such reasons are obvious, unsurprising, and, in many regards, understandable.

However, in modern industrialized democracies—such as the United States—businesses have not been able to make absolute assertions of secrecy. Generally speaking, for the privilege of operating in the marketplace, businesses provide certain information to government as the regulator of social and economic intercourse. Justice Brandeis made this same point over fifty years ago in the following memorable words:

> Whether the corporate privilege shall be granted or withheld is always a matter of state policy. If granted, the privilege is conferred in order to achieve an end which the State deems desirable.[1]

From this situation there arises a condition of continuous tension as to the kinds and quantities of business information that are provided to government as well as the arrangements under which it is obtained, maintained, and utilized by agencies of the state.

Harold C. Relyea is a specialist in American National Government, Congressional Research Service, Library of Congress, Washington, D.C.

Furthermore, government may make general rules for society regarding the privileged status of different kinds of business information. The unauthorized disclosure of proprietary knowledge or "trade secrets," for example, might be made punishable through the judicial process. Conversely, temporary exclusive use of information about a device or machine might be granted to an inventor provided it is available for public use after a particular period of time.

Businesses in the United States devote considerable resources to secrecy matters. Billions of dollars are spent each year on "industrial security" arrangements to safeguard information. But probably as much, if not more, is allocated annually to intelligence endeavors for gathering information about competitors. And armies of attorneys, lobbyists, and publicists are regularly retained to plead the cause of business control of business information, to check potential public-policy changes threatening business information protection, and to monitor and, if necessary, challenge government institutions attempting to disclose business information.

What is explored here are the contexts in which secrecy is applied to business information as a matter of public policy. However, some theoretical and conceptual caveats are in order. The overview is, as the title suggests, confined to policies and practices of the U.S. federal government. Further, lest the title be misunderstood, there is no single, unified national commercial information policy. This is a generic reference. There are, of course, a variety of federal commercial information policies that are sometimes related.

Next, a few words about the concept of *secrecy*. The defining trait or characteristic of secrecy, as Sissela Bok notes, is concealment or hiding.[2] An important consideration in this discussion is the extent to which concealment can be realized by businesses. Bok also points out that this understanding of the term is a neutral one which does not assume "that secrets are guilty or threatening, or on the contrary, awesome and worthy of respect."[3] This perspective has guided the analysis offered here, but does not necessarily underlie the policies under examination. When Edward Shils defines secrecy as "the compulsory withholding of knowledge, reinforced by the prospect of sanctions for disclosure,"[4] we are reminded that policymakers, indeed, have made judgments that certain applications of secrecy to information must be respected or punishments shall ensue.

Then, we come to the object of secrecy—*business information*. It was said at the outset that businesses in the United States seek control over information concerning their sales and the production of what they are selling. The reference to sales and production information is broadly

interpreted here. And the seeking of control over information is described, as a matter of emphasis, as "a condition of continuous tension." Thus, businesses are continuously attempting to make or keep secret that information which they determine to merit protection. In law or public policy affording some type of secrecy, definitions or characterizations of this information may be subject to administrative interpretation or susceptible to modification through litigation. Recognizing these somewhat unsettled conditions, it has been said that what is explored here are the contexts in which secrecy is applied to business information as a matter of public policy. In brief, there are, as will be seen, various and changing understandings of "business information" in federal law and policy.

Finally, our subject matter certainly lends itself to more analysis and exploration than is offered here.[5] To reiterate, this discussion is a general overview and, as such, it does not purport to be definitive or exhaustive. Space considerations alone posed a practical limitation. Nonetheless, it is hoped that a useful treatment has resulted.

The Privacy Threshold

There can be little doubt that privacy—the autonomous determination of when, how, and to what extent information about oneself is communicated to others—has become an increasingly important and cherished value in American society. And, from time to time, assertions are heard that businesses—particularly corporations as *personae fictae*—are entitled to privacy protections equal to those afforded by the law as personal privacy rights. However, without detailing these analogous protections, it is sufficient to say that this contention has not gained acceptance. As one witty jurist once stated the prevailing view, "if you don't have any privates, you're not entitled to any privacy."

A century ago, the Supreme Court recognized corporations as being "persons," but has not vested them with the privacy rights reserved for individuals.[6] Edward Shils described privacy some years ago as "the voluntary withholding of information reinforced by a willing indifference."[7] In this context, perhaps businesses or corporations may lay a claim to a privacy interest. However, during the past few decades, the voluntary withholding of information has broken down in the face of increased regulatory and verification demands, more rigorous surreptitious collection efforts, and the skillful application of new technology in these matters. As a result, both individuals and organizations have sought protection in the law. "The lack of privacy for certain core secrets," Alan F. Westin has observed, "can threaten the independence

or autonomous life of an organization much as it does that of an individual."[8]

Whether privacy is effectively enjoyed by both individuals and businesses in the United States may be, to some extent, a matter of definition. However, they do not enjoy equal privacy rights. Generally, when legal protection has been accorded to the information of businesses, it has been done for economic reasons and without explanation in terms of privacy rights. By contrast, the protection of individuals' personal privacy has been based upon human values and traits with specific identification of several privacy rights rooted in the Constitution.[9] In sum, there are more appropriate and perhaps more important concepts than privacy to be considered when assessing the contexts in which secrecy is applied to business information as a matter of public policy.

Trade Secrets

If there is a jewel in the crown of business information protection it is the law of trade secrets. The concept of a trade secret is not well defined or, perhaps better stated, its definition is not a commonly agreed upon understanding. Flexibility in interpretation is desirable so that new technologies and intellectual endeavors may be accommodated by the term and its underlying protective status. Probably the most widely accepted statement of what constitutes a trade secret is found in the *Restatement of Torts* which, in part, says: "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."[10]

Given the somewhat loose nature of the trade secret concept, it should not be surprising that the law of trade secrets is rather pliable. It is largely judge-made, although there are some state and federal statutes providing remedies against the disclosure of trade secrets. And it is in the common-law tradition, arising from usages and customs of immemorial antiquity and from the judgments and decisions of the courts recognizing, affirming, updating, and enforcing such past practices.

Historically, the law of trade secrets arose from a concern about commercial ethics. In brief, its purpose is largely to enforce standards of fair play in business conduct. There are, therefore, certain expectations that must be met in order that judicial protection or a statutory remedy may apply. First, it must be demonstrated that the information in question constitutes a trade secret—that it is used in one's business, provides a competitive advantage, and is exclusively held. Second, it

must be shown that reasonable precautions were taken to prevent the information from becoming known by "proper" means. Third, the secrecy breach must be established: the information was obtained by "improper" means or in violation of a contractual or fiduciary obligation.

There are several secrecy considerations worth mentioning at this juncture. First, depending upon the circumstances, a business may not seek recovery for the loss of a trade secret for fear that, in the course of a judicial proceeding, more details about the trade secret at issue might have to be disclosed or other confidential commercial information might have to be revealed. Protective orders, of course, may be a mitigating factor. Nevertheless, the situation serves to explain why trade secrets may be closely held by a selective few within a business and also why litigation directly addressing loss of trade secrets is not always pursued, particularly when some other prosecutorial strategy of less commercial risk might be available.

This brings us to the second and third pertinent secrecy considerations. Although the law of evidence affords trade secrets a privilege from routine disclosure in litigation, it is not an absolute protection. In order to have a fair trial, judges have ordered the production of documents and testimony involving trade secret information. The privilege is, therefore, a qualified one.

Third, businesses have found contracts and agreements to be a useful and effective way to protect trade secrets. Certainly for practical reasons, physical safeguards, compartmentalization of knowledge, and the close holding of information by a selective few are not always sufficient or adequate. A nondisclosure contract not only provides an element of flexibility in security arrangements, but also offers an alternative, and perhaps less risky, prosecutorial strategy for punishing trade secret losses. In brief, a business may find it more desirable to pursue a breach of contract lawsuit than to litigate directly on expropriation of a trade secret.

Finally, it should be apparent from the foregoing paragraphs that trade secrets are a peculiar kind of secret. In fact, the term is something of a misnomer. Trade secrets are often widely known. As a consequence of nondisclosure contracts, a great many employees in a particular business may be exposed to its trade secrets. Through licensing arrangements, a corporation may reveal trade secrets to another firm. And certainly more than one business has become aware that a competitor, through independent initiative, possesses and uses a trade secret which is not its exclusive knowledge.

It is difficult to say, with any degree of certainty, what the attractiveness of the trade secrets system is vis-à-vis, for example, the patent arrangement. One attribute would appear to be the general flexibility of trade secrets law. But, while this consideration attests to the need to accommodate new production processes and technology, another attraction of trade secrets safeguards may be their propensity for preserving the status quo. This occurs partly because trade secrets arise from a common-law tradition and partly because of an acceptance of the secrecy myth attending this particular type of knowledge. Trade secrets are protected as a consequence of custom and past practice, and also because they stand *sui generis* as business information actually used in production and providing a competitive advantage. A great deal of the character of trade secrets rests with their status of being a veiled secret.

Patent Protection

By contrast, information protected under federal patent law has the status of being an open secret. The situation is nicely described by a line from the third act of *Man and Superman* when Shaw has one of his characters say: "We shall never be able to keep the secret unless everybody knows what it is."

A patent is a seventeen-year right of exclusive use given to an inventor in exchange for the disclosure of the invention so that it will be available for free public use when the patent period expires.[11] Like trade secrets law, patenting grew out of concern for commercial ethics and seeks, as well, to provide incentives for innovation. The Republic of Venice is credited with enacting the first patent law in 1474. Such a statute initially appeared in the United States in 1641 as a consequence of legislative action taken in the Massachusetts Bay Colony.[12] When the federal Constitution was ratified in 1788, it specifically empowered Congress, in Article I, Section 8, Clause 8, "To promote the Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[13] The first federal patent law was subsequently enacted in 1790.[14]

As might be anticipated, inventors, lawyers, and judges have found interpretation of the patent statute and resolution of patent lawsuits inordinately difficult. A few years ago, Justice Byron White commented in an opinion "that patent litigation can present issues so complex that legal minds, without appropriate grounding in science and technology, may have difficulty in reaching decision."[15]

Under current patent arrangements, all the information in a patent application is held in confidence by the Patent and Trademark Office of the Department of Commerce until the patent actually issues. Approved patent applications may be inspected, but the information may not be utilized during the patent period except through licensing with the holder. Patent infringement or piracy may be pursued in court. However, this kind of litigation, as noted earlier, is highly complex, often prolonged, and usually expensive. For several reasons, patenting is less desirable than trade secrets protection. Nevertheless, there are certain types of inventors who find these arrangements quite suitable for their purposes. Universities and small businesses, for example, may not be prepared to maintain a trade secret or otherwise may regard patenting a better way to realize profit through the licensing or sale of the patented information. Also, in an area of rapid development, an inventor may consider seventeen-year exclusive use adequate, knowing that by the time the protection period lapses, innovation will provide patentable enhancements on the original invention or some other improvement making it obsolete.

Regarding the shift away from patenting, Russell Stevenson recently wrote that, "while the empirical evidence is scanty, it appears that reliance on trade-secret protection is increasing, and in many cases even where inventions meet the standards of patentability."[16] He offers a number of reasons for this phenomenon. First, it is more expensive to acquire and defend a patent than to keep a new technological development protected by trade secrets arrangements. Second, in addition to cost considerations, the law of trade secrets is thought to be more successful in safeguarding proprietary information. Third, because approved patent applications are subject to public scrutiny, there is a preference for the security afforded by trade secrecy. Finally, there are innovations that simply are not patentable.[17]

There is one other aspect of the patent system that some might find repugnant and perhaps threatening. This is the possibility that the government might seize a patent application, divert it from being the basis for an open secret, and impose in its stead an order for absolute secrecy. How does this happen?

Shortly after the United States entered World War I, Congress provided authority for the Commissioner of Patents[18] or the president[19] to withhold certain patents the publication of which might "be detrimental to the public safety or defense, or may assist the enemy or endanger the successful prosecution of the war," in order to keep the invention in question secret. Congress broadened the Patent Commissioner's powers in this area in 1940 by deleting the requirement that the

United States be at war and by allowing the commissioner to so withhold the grant of a patent "for such period or periods as in his opinion the national interest requires."[20] This general authority lasted until the end of World War II.[21] However, a permanent statute on this matter was subsequently enacted in 1952.[22]

The Invention Secrecy Act currently provides that "whenever the publication or disclosure of an invention by the granting of a patent, in which the Government does not have a property interest, might, in the opinion of the [Patent] Commissioner, be detrimental to the national security," he shall make the application available to certain specified defense agencies for review. In the event that one of these defense agencies determines that "the publication or disclosure of the invention by the granting of a patent therefor would be detrimental to the national security,...the Commissioner shall order that the invention be kept secret and shall withhold the grant of a patent" for not more than one year, subject to a possible renewal.[23] These secrecy restrictions may be appealed to the Secretary of Commerce[24] and a claim for compensation for the damage caused by such a secrecy order may be made through the proper federal court.[25]

Although patent secrecy orders are not applied to a large quantity of independently developed innovations, their effect is decisive. An inventor subject to such an order who willfully publishes or discloses the information it covers not only forfeits his patent right but also can be fined $10,000 or imprisoned for two years, or both.[26] The affected proprietary information is not usable. Compensation is difficult to obtain and usually no details are provided regarding the national security detriment prompting the government's action.[27]

Statutory Protection

The law of trade secrets and patenting arrangements are two major ways in which secrecy is applied to business information as a matter of public policy. As the discussion indicates, neither system affords absolute protection. They are designed to facilitate fair commercial practice in the marketplace. Because it is a marketplace subject to government scrutiny and regulation, there is a necessity for the government to obtain various kinds of business information. In this regard, there arise additional contexts in which secrecy is applied to business information as a matter of public policy.

Both Congress and the federal courts have discretionary authority for protecting business information. Congressional committees may invoke their rules for an executive session and receive business informa-

tion in a closed proceeding or as if they were conducting a secret meeting. Similarly, a federal judge, as mentioned earlier, may issue a protective order limiting the availability of business information introduced in conjunction with or during a court hearing.

The federal departments and agencies are subject to various statutes governing the protection of business information. There is a criminal code provision which prohibits officers and employees of the executive branch from publishing, divulging, disclosing, or making known "in any manner or to any extent not authorized by law" any information received during the course of their employment concerning or relating to trade secrets or certain similar specified information.[28] In addition, there is a category of laws requiring absolute protection of proprietary information by the departments and agencies, and another group mandating qualified safeguarding. All of these authorities will be examined shortly. And there are also the exemptions to the rule of information disclosure of the Freedom of Information Act (FOIA).[29] This statute will be considered in a separate, succeeding section.

The federal criminal law prohibition of agency disclosure "in any manner or to any extent not authorized by law" of trade-secret type information was enacted in 1948 as one small section of a codification statute. The section has come to be known as the Trade Secrets Act. Its legislative history indicates that three similar provisions appearing in the 1940 edition of the *U.S. Code*—one from an income tax statute,[30] one from a tariff commission law,[31] and one from a commerce department authority[32]—were consolidated to create the new section. According to one analyst, the underlying legislative history "nowhere hints that Congress sought to alter substantively the reach of the three nondisclosure statutes."[33] However, the language of the new section, taken literally, sweeps far more broadly than the original three provisions from which it arose. Further, it appears that the courts "have applied an overly broad interpretation of the section."[34] Thus, the Trade Secrets Act has come to be viewed as having effect throughout the executive branch.

It has been said, quite properly, that the language of the section "encompasses virtually every category of business information in agency files."[35] And the effect of the act is to punish criminally any officer or employee of the United States disclosing such information "in any manner or to any extent not authorized by law." Unfortunately, the understanding of the nature of the qualified exception to the section's rule of nondisclosure has been made difficult because Congress did not define the phrase "authorized by law" or indicate if disclosure might be "authorized" by agency regulations. An even more difficult question

concerns the relationship of the Trade Secrets Act to the Freedom of Information Act.

For our purposes, some clarifications in this situation may be found in the Supreme Court's 1979 ruling in the *Chrysler* case.[36] Here it was affirmed that "properly promulgated, substantive agency regulations" have the force and effect of law in a variety of contexts, including the Trade Secrets Act.[37] According to the Administrative Procedure Act, a "substantive" regulation or rule is distinguished from "interpretive rules, general statements of policy, or rules of agency organization, procedure, or practice."[38] Noting this distinction, the *Chrysler* opinion indicated that a substantive or "legislative-type rule" is one "affecting individual rights and obligations," a characteristic which the Court deemed "an important touchstone for distinguishing those rules that may be 'binding' or have the 'force of the law.' "[39] In order to have binding effect, substantive regulations, said the Court, must be "issued by an agency pursuant to statutory authority" and their promulgation "must conform with any procedural requirements imposed by Congress," such as those found in the Administrative Procedure Act.[40]

The Court then confined itself to a rather limited treatment of the relationship between the Trade Secrets Act and the Freedom of Information Act. "Since materials that are exempt from disclosure under the FOIA are...outside the ambit of that Act," said the *Chrysler* opinion, "the Government cannot rely on the FOIA as congressional authorization for disclosure regulations that permit the release of information within the Act's nine exemptions."[41] However, because of the conditions of the case at issue, the Court did not find it necessary to make any further determinations regarding the relationship of the two statutes.[42] Thus, there was no judgment regarding the question of whether or not the Trade Secrets Act constitutes a nondisclosure law falling within the third exemption of the FOIA.[43] Indeed, although there was much authoritative opinion rejecting the contention that the Trade Secrets Act was an exemption 3 statute, the *Chrysler* decision may have rekindled support for the viewpoint.[44] The Court also chose to render no opinion as to the relationship between the Trade Secrets Act and the fourth exemption of the FOIA pertaining to trade secrets and confidential commercial information.[45]

In view of the Supreme Court's determination in *Chrysler* that a substantive regulation, in part, must be "issued by an agency pursuant to statutory authority" in order to be binding or have the force of law, it is now appropriate to explore the different kinds of statutes providing absolute or qualified protection for business information held by federal departments and agencies.[46] There are various statutory provisions

in the *U.S. Code* and uncodified laws that impose a general prohibition, without exceptions, on the disclosure of proprietary business information obtained during the course of agency operations. For example, in conducting an official investigation, the Commodity Futures Trading Commission "may publish from time to time, in its discretion, the result of such investigation and such statistical information gathered therefrom as it may deem of interest to the public, except data and information which would separately disclose the business transactions of any person and trade secrets or names of customers."[47] The Federal Trade Commission is similarly barred from making public "trade secrets and names of customers."[48]

There are also a number of statutory provisions that impose a general prohibition on the disclosure of certain business information, but allow an exception to this rule for Congress and/or congressional committees. For example, there are several such protective provisions which conclude with the following statement or a closely similar phrase: "Nothing in this section shall authorize the withholding of information by the Secretary or any officer or employee under his control from the duly authorized committees of the Congress."[49]

Further, there are various statutory provisions that impose a general prohibition on the disclosure of certain business information, but allow a specific exception for disclosure in any relevant administrative or judicial proceeding authorized by statute. The language in a pertinent section of the Flammable Fabrics Act is rather common phrasing on this point, indicating that "such information may be disclosed to other officers or employees concerned with carrying out this chapter or when relevant in any proceeding under this chapter."[50] The Hazardous Substances Act makes allowance for the revealing of protected business information "to the courts, when relevant in any judicial proceeding under this chapter."[51] And prohibitions on the disclosure of poultry inspection[52] or egg products inspection information[53] entitled to protection as a trade secret make allowance for revelation "as ordered by a court in any judicial proceeding."

There are a few statutory provisions that vest discretionary authority to protect trade secrets in the head(s) of an agency and require the supplier of sensitive business information to request its protection as a trade secret. The Securities and Exchange Commission, for example, exercises such authority regarding certain information filed by public utility holding companies. Suppliers of this information may make written objection to its disclosure, "stating the grounds for such objection, and the Commission is authorized to hear objections in any such

case where it finds it advisable."[54] Similarly, certain exempt organizations and certain trusts may request that the Secretary of the Treasury or his delegate withhold from public inspection some supporting papers to their tax exemption applications. The secretary or his delegate must determine if the information at issue "relates to any trade secret, patent, process, style of work, or apparatus of the organization" and that "public disclosure of such information would adversely affect the organization."[55]

There are also a few statutory provisions that allow an agency head to disclose confidential information, including business information, if necessary, to carry out the purposes of a statute or in the interest of public health and safety. Examples of this authority may be found in provisions concerning certain weather information,[56] electronic product radiation,[57] and boating safety.[58]

Finally, there are some statutory provisions that allow the exchange of confidential information, including business information, between federal agencies. For example, pesticide,[59] vehicle emission,[60] and noise data[61] are governed by such law. And in carrying out certain of his duties, the Secretary of Transportation is authorized to request pertinent information, including confidential business information, from other federal departments and agencies which are "authorized and directed to cooperate with the Secretary and furnish such information."[62]

Freedom of Information Act

In addition to the types of statutory provisions discussed earlier which afford varying degrees of protection for business information, there is one other law that provides a measure of safekeeping for business records, but does so in the context of presumptive disclosure. Originally enacted in 1966, the Freedom of Information Act provides the public with legal authority and a procedure to obtain records held in agency files.[63] Such records, of course, might have been submitted by a business or otherwise might contain sensitive proprietary data. Any person, including a business, may request these materials pursuant to the FOIA. An agency may decline to provide requested records by relying upon exemptions to the rule of disclosure specified in the FOIA. Two of these, the third and the fourth exemptions, have particular pertinence for business information.[64]

Businesses do use the FOIA to attempt to obtain information about competitors. And while no business wants details about its operations and products disclosed in this way, there apparently is also a degree of

feeling within the business community that such FOIA requests are not improper. In a recent oversight hearing, the chairman of a Senate subcommittee queried a witness representing the U.S. Chamber of Commerce about the propriety of this practice, calling it "an abuse of the intent of the act." The witness responded, saying:

> I would respectfully disagree with you in that I do not feel that the use of the Freedom of Information Act in the manner that you have just described is necessarily an abuse of the act. During the Congress deliberations over what became the Freedom of Information Act, it expressly rejected the notion of a right to know or a need to know in order to take advantage of the legislation. So what you have described as abuse, in fact represents adaptness and proficiousness in the use of the act.[65]

In 1984, there were 281,102 reported FOIA requests,[66] which was a notable increase over the 262,265 request volume of the previous year.[67] Although precise information on the point is not available, probably 50 to 60 percent of these requests are attributable to the business community (i.e., corporations, businesses, legal representatives, or other commercial representatives). However, this does not mean that these requests resulted in the disclosure of any information of entrepreneurial value to the requester or, conversely, that valuable proprietary data were lost to a competitor. Indeed, it appears that the FOIA is not a very useful tool for conducting industrial espionage. Nonetheless, the business community continues to have anguish and anxiety about disclosures of its information pursuant to the FOIA.

Businesses can attempt to prevent an agency from releasing proprietary information that is arguably protectable under one or more of the exemptions of the FOIA. In the *Chrysler* case, the Supreme Court ruled that the exemptions of the FOIA are not mandatory and neither that statute nor the Trade Secrets Act provides a private right of action to prevent agency disclosure of information.[68] However, the Court indicated[69] that judicial review of agency action in these matters is available to submitters of business records under the Administrative Procedure Act.[70] Also, in the aftermath of the *Chrysler* decision, many agencies established procedures for notifying business submitters when their records were being sought pursuant to the FOIA and providing an opportunity for them to argue against the release of such material.

While these procedural arrangements are valuable to the business community, serious interpretive problems arise from FOIA exemptions three and four. In the case of the third exemption, there is the question of appropriate statutory provisions that meet the criteria of the exception clause. The situation is somewhat more difficult regarding the fourth

exemption covering "trade secrets and commercial or financial information obtained from a person and privileged or confidential." In a 1967 interpretive memorandum on the FOIA, the attorney general commented:

> The scope of this exemption is particularly difficult to determine. The terms used are general and undefined. Moreover, the sentence structure makes it susceptible of several readings, none of which is entirely satisfactory.[71]

Summarizing the dilemma as it has subsequently evolved, Russell Stevenson notes "there is no generally agreed definition of what constitutes a 'trade secret,'" and adds that "the second part of the exemption, for 'commercial or financial information,' has left more than ample latitude for the protection of commercially sensitive information that does not relate to the technical details of a manufacturing process."[72] The difficult question then arises as to when information should be considered "privileged and confidential?" Generally accepted judicial guidance on this point comes from the *National Parks* case: information is "confidential" within the terms of the fourth exemption if disclosure would either (1) impair the ability of the government to obtain similar such information in the future, or (2) "cause substantial harm to the competitive position of the person from whom the information was obtained."[73] Although it has been somewhat difficult to determine what "substantial harm to the competitive position" of a submitter means, the courts, notes Stevenson, "have imposed the burden of showing some injury on the private party who has supplied the information and seeks to prevent its release" and required "more than unsupported, conclusory allegations of potential harm."[74] This interpretative dilemma in litigation to prevent agency disclosure of submitters' business information has resulted in what Stevenson calls, with a bit of understatement, "varying and inconsistent results."[75] And while many businesses are probably not pleased with this situation, its unsettled status offers hope that a favorable public policy will subsequently result.

Conclusion

This brief overview has generally explored the contexts in which secrecy is applied to business information as a matter of public policy. The situation is a fluid one, with businesses vying with each other for information to improve their market standing. It is also a situation filled with dynamics, including continuous tension as to the kinds and

quantities of business information that are provided to government as well as the arrangements under which it is obtained, maintained, and utilized by agencies of the state. Businesses are continuously attempting to make or keep secret that information that they determine to merit protection. They are understandably satisfied when the balance of favor in public policy leans toward protection. Conversely, of course, their anxieties arise and mount in the face of public policy disposed toward disclosure.

But, to what extent is secrecy—effective concealment or hiding—actually being realized in these matters? Indications are that what businesses have attained in public policy regarding their proprietary information is not *secrecy*, but *control* over its disclosure. In their separate ways, the law of trade secrets, licensing arrangements, and patenting provide this control. And when business information is turned over to federal agencies, statutes, in varying degrees, exert this control. The Freedom of Information Act poses a threat because the business community is presently uncertain about the measure of control that may be exercised to check agencies' decisions to disclose business information pursuant to the statute.

Some might argue with this change in characterization or contend that it is a distinction without a difference. However, it appears that the term *secrecy* functionally is not an accurate descriptor, but has important symbolic value in these matters. Indeed, if law and public policy give recognition to business information as a secret, reinforced by sanctions for disclosure, who shall not honor its privileged status?

Note: The views expressed in this article are those of the author and are not attributable to any other source.

References

1. *Louis K. Liggett Company* v. *Lee*, 288 U.S. 517, 545 (1933).
2. Bok, Sissela. *Secrets*. New York: Pantheon Books, 1982, p. 6.
3. Ibid., p. 9.
4. Shils, Edward A. *The Torment of Secrecy*. Glencoe, Ill.: The Free Press, 1956, p. 26.
5. See Stevenson, Russell B., Jr. *Corporations and Information: Secrecy, Access, and Disclosure*. Baltimore, Md.: Johns Hopkins University Press, 1980; and of related interest is Goldschmid, Harvey J., ed. *Business Disclosure: Government's Need to Know*. New York: McGraw-Hill, 1979.
6. See *Santa Clara County* v. *Southern Pacific Railroad Company*, 118 U.S. 394 (1885); and also see *California Bankers Association* v. *Schultz (Secretary of the Treasury)*, 416 U.S. 21, 65 (1974), quoting *United States* v. *Morton Salt Company*, 338 U.S. 632, 651-52 (1950).
7. Shils, *The Torment of Secrecy*.

8. Westin, Alan F. *Privacy and Freedom.* New York: Atheneum, 1970, p. 43. See also Gross, Bertram M. *The Managing of Organizations,* vol. II. New York: Free Press of Glencoe, 1964, pp. 732-33. Perhaps one indication of Westin's thinking about organizational privacy may be found in *NAACP* v. *Alabama,* 357 U.S. 449 (1958). Regarding other privacy interests associated with corporate files, see Stevenson, *Corporations and Information,* pp. 70-73.

9. See *Griswold* v. *Connecticut,* 381 U.S. 479 (1965); and Clark, R.H. "Constitutional Sources of the Penumbral Right to Privacy." *Villanova Law Review* 19(June 1974):833-84.

10. American Law Institute. *Restatement of Torts,* vol. 4, sec. 757, comment b. St. Paul, Minn.: American Law Institute, 1939, p. 5.

11. See 35 U.S.C. 100-73, 251-61, 271-94.

12. Stevenson, *Corporations and Information,* p. 17.

13. The origins of copyright law also rest in this constitutional provision.

14. 1 Stat. 109, chapter VII.

15. *Blonder-Tongue Laboratories, Inc.* v. *University of Illinois Foundation,* 402 U.S. 313, 331 (1971).

16. Stevenson, *Corporations and Information,* p. 21.

17. Ibid., pp. 21-22.

18. 40 Stat. 394.

19. 40 Stat. 442.

20. 54 Stat. 710.

21. See 56 Stat. 370.

22. See 66 Stat. 3; and 66 Stat. 792 at 805.

23. See 35 U.S.C 181-88.

24. 35 U.S.C. 181.

25. 35 U.S.C. 183.

26. 35 U.S.C. 186.

27. See, generally, U.S. Congress, House Committee on Government Operations. *The Government's Classification of Private Ideas.* H. Rep. 96-1540, 96th Cong., 2d sess. Washington, D.C.: USGPO, 1980, pp. 1-62.

28. 18 U.S.C. 1905.

29. See 5 U.S.C. 552(b)(1)-(9).

30. 18 U.S.C. 216 (1940).

31. 19 U.S.C. 1335 (1940).

32. 15 U.S.C. 176a (1940).

33. Clement, Daniel Gorham. "The Rights of Submitters To Prevent Agency Disclosure of Confidential Business Information: The Reverse Freedom of Information Act Lawsuit." *Texas Law Review* 55(March 1977):614.

34. Ibid., p. 613.

35. Ibid., p. 603.

36. *Chrysler Corporation* v. *Brown,* 441 U.S. 281 (1979).

37. Ibid., pp. 295, 301.

38. 5 U.S.C. 553(b), (d).

39. *Chrysler Corporation* v. *Brown,* 441 U.S. 301-02, citing *Morton* v. *Ruiz,* 415 U.S. 199 (1974).

40. *Chrysler Corporation* v. *Brown,* 441 U.S. 302-03.

41. Ibid., pp. 303-04.

42. See ibid., p. 319, note 49.

43. 5 U.S.C. 552(b)(3) (the third exemption to the Freedom of Information Act's rule of disclosure pertains to records "specifically exempted from disclosure by statute..., provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld").

44. See, for example, *Guerra* v. *Guajardo,* 466 F. Supp. 1059 (S.D. Tex. 1978); *Florida Medical Association, Inc.* v. *Department of Health, Education and Welfare,* 479 F. Supp. 1291 (M.D. Fla. 1979); *Westchester General Hospital, Inc.* v. *Department of Health, Education and Welfare,* 464 F. Supp. 236 (M.D. Fla. 1979). Cf. *Burroughs Corp.* v. *Brown,* 501 F. Supp. 375, 382-83 (E.D. Va. 1980).

45. 5 U.S.C. 552(b)(4) (the fourth exemption to the Freedom of Information Act's rule of disclosure pertains to "trade secrets and commercial or financial information obtained from a person and privileged or confidential").

46. This effort was assisted by Ehlke, Richard. *Federal Protection of Trade Secrets and Proprietary, Commercial and Financial Information Obtained By Government Agencies in the Context of Energy-Related Data* (Congressional Research Service Report 77-226A 654/126, 13 Oct. 1977). Washington, D.C.: USGPO, 1977.

47. 7 U.S.C. 12.

48. 15 U.S.C. 46(f).

49. 15 U.S.C. 1193(c), 1401(e), 1402(b)(2), 1944(f), 2055(a)(2).

50. 15 U.S.C. 1193(c).

51. 15 U.S.C. 1263(h).

52. 21 U.S.C. 458(a)(5).

53. 21 U.S.C. 1037(e).

54. 15 U.S.C. 79v.

55. 26 U.S.C. 6104(a)(1)(D).

56. 15 U.S.C. 330b(c)(3).

57. 42 U.S.C. 263g(d).

58. 46 U.S.C. 1464(d).

59. 7 U.S.C. 136h.

60. 42 U.S.C. 1857f-6(b).

61. 42 U.S.C. 4912(b).

62. See 15 U.S.C. 1914(c)(1), 1943(a).

63. The Freedom of Information Act was intially passed in 1966 (80 Stat. 250), codified the following year (81 Stat. 54), significantly amended in 1974 (88 Stat. 1561), and modified in a minor way in 1976 (90 Stat. 1247). It appears in the U.S. Code at 5 U.S.C. 552.

64. See notes 43 and 45 *supra.*

65. U.S. Congress, Senate Committee on Governmental Affairs, Subcommittee on Intergovernmental Affairs. *Oversight of the Administration of the Federal Freedom of Information Act.* Hearings, 96th Cong., 2d sess. Washington, D.C.: USGPO, 1980, pp. 150-51.

66. See *Access Reports* 11(11 Sept. 1985):4.

67. See *Access Reports* 10(29 Aug. 1984):4.

68. *Chrysler Corporation* v. *Brown,* 441 U.S. 281 (1979).

69. Ibid., p. 317.

70. 5 U.S.C. 702.

71. U.S. Department of Justice. *Attorney General's Memorandum on the Public Information Section of the Administrative Procedure Act.* Washington, D.C.: U.S. Dept. of Justice, June 1967, p. 32.

72. Stevenson, *Corporations and Information,* p. 178.

73. *National Parks and Conservation Association* v. *Morton,* 498 F.2d 765, 770 (D.C. Cir. 1974).

74. Stevenson, *Corporations and Information,* p. 179.

75. Ibid., p. 181.

This Page Intentionally Left Blank