Commercial satellite imagery: CI, KM, and trade secret law

Cynthia M. Gayton
School of Engineering and Applied Sciences, The George Washington University, Washington, District of Columbia, USA

Abstract

Purpose – The purpose of this paper is to examine the implications of remote surveillance or satellite imagery as they relate to trade secret law, knowledge management, and competitive intelligence.

Design/methodology/approach – The paper approaches legal issues from the perspective of a trade secret holder.

Findings – While conducting research for this paper, it was found that, while technological improvements relating to satellite imagery and remote sensing are increasingly more precise and ubiquitous, the laws protecting businesses that have an interest in protecting trade secrets are inconsistent. On the one hand, the US Government has given itself a powerful tool to protect trade secrets under the Economic Espionage Act. On the other hand, the Government has granted remote satellite companies licences under which they may sell satellite images to industrial competitors, consequently thwarting trade secret protection efforts

Originality/value – Trade secrets represent a valuable contribution to a nation's economy, particularly when some interventions do not meet the requirements necessary for more traditional intellectual property regime protection (e.g. copyright, trade mark, patents). A trade secret's value lies in it remaining hidden. There are few cases addressing trade secrets and satellite imagery. The stalwart case, *E.I. duPont deNemours & Co., Inc.* v. *Rolfe Christopher*, represents a tentative foray into the subject, but only suggests the rights a trade secret holder may have when a commercial satellite company collects otherwise innocuous data and sells those to a competitor. A proper plaintiff to test the boundaries surrounding trade secret law, satellite imagery, and competitive intelligence remains at large.

Keywords Law, Artificial satellites, Surveillance, Knowledge management, Trade secrets

Paper type Conceptual paper

> This is a case of industrial espionage in which an airplane is the cloak and a camera the dagger (Judge Goldberg, *E.I. duPont deNemours & Co., Inc.* v. *Rolfe Christopher*).

The impetus for this article was a question posed from one of my students as I breezed through the intellectual property portion of my engineering law course. When we got to trade secrets, I briefly described an old chestnut of a case, *E.I. duPont deNemours & Co., Inc.* v. *Rolfe Christopher*, to outline the reasonable efforts necessary to maintain the confidential nature of a trade secret. In the case, photographers in a plane flew above duPont's Beaumont, Texas, plant, took photos and sold them to an unknown third party. The photographers, not their undisclosed client, were sued. The court found the photographers guilty of misappropriation of trade secrets. One student, upon hearing this conclusion, was particularly concerned about how the case would apply to a company that provided satellite images of sensitive sites. Specifically, if a company in

VINE: The journal of information and knowledge management systems
Vol. 37 No. 2, 2007
pp. 192-206

0305-5728
DOI 10.1108/03055720710759964

the business of supplying satellite images for competitor intelligence purposes sold these satellite images (which could reveal otherwise trade secret protected information), would that company be liable for trade secret misappropriation? My carefully considered knee-jerk response was if the client or the person who collected the images was in a position to know that the target intended to keep information secret, and, in fact, the company had made reasonable efforts to keep that information secret, despite the satellite image's public availability, there may still be a cause of action for a trade secret violation. Fortunately, the class period ended and we moved on to products liability.

But the question remained with me. If my statement was true, who would be sued? The company that used the information readily available in the public domain[1]? Is this a trade secret issue or a privacy issue? This article reflects my research into this area. First, I will explore the progression of intellectual property rights from their virtual non-existence to their becoming a derivation of physical property rights from a quasi-historical/contextual perspective. Second, I will compare various trade secret definitions and the laws that protect trade secrets. Because the acquisition of competitor information borders on knowledge management and competitive intelligence, I will next compare knowledge management systems to competitive intelligence. Fourth, and finally, I will set up a hypothetical situation with which to address my student's question.

1. The abstraction of intellectual property

Copyright, patent, trademark and trade secret protection represents the results of a progressive abstraction of intellectual property rights. Ben-Atar (2004) discussed this progression in his book *Trade Secrets*. In Table I, I present in what he describes in his book, which I hope will be a useful framework to begin my analysis.

Note that starting with the Early Modern Europe period, the protection enjoyed by the rights holder is rewarded for invention, discovery or acquisition regardless of whether there is a "product". For example, today one can hold a patent revealing to the public the best methods to produce a nuclear weapon. However, federal, state or international law may forbid the actual reduction of the patent to practice, i.e. to create a product. Similarly, trade secrets have value only because they are not revealed to the public; hence, few may ever know what the trade secret protects.

2. What are trade secrets?

Trade secrets, as protected intellectual property, are inherently more abstract than any other federally protected intellectual property because they never have to be disclosed to the public. Copyrights and patents in particular are subject to time limitations under which the government will grant protection. Trademarks may be protected for as long as the mark is used in commerce[2]. This implies that there is no presumption that the public will ever benefit from the revelation of, or be permitted to use, a trade secret, because, by definition, in order to maintain its status as a trade secret, it must not be generally known[3]. In fact, the public derives its benefit solely from the services provided under the trade secret[4].

Historic period	Knowledge and value embodiment	Protection granted	Protective/reward/enforcement
Ancient world	Object itself[a]	None	Theft/plagiarism
Early Renaissance	Skill	None	Guilds regulated access to knowledge of process and operation of machines[b]
Early Modern Europe	Individual innovator	Temporary monopoly	Cash rewards to inventors, cause of action against infringers
Modern	Practical application/socially useful	Explicit (and sometimes temporary) monopoly in the form of patents, trade marks, trade secrets, copyright	Cause of action against infringers (statutory damages, if registered; attorney's fees; injunctive relief; recovery of ill-gained profits)

Notes: [a]Heidegger describes the ancient world's understanding of the essence of a thing as well as what technology is as follows: "According to ancient doctrine, the essence of a thing is considered to be *what* the thing is. We ask the question concerning technology when we ask what it is. Everyone knows the two statements that answer our question. One says: Technology is a means to an end. The other says: Technology is a human activity. The manufacture and utilization of equipment, tools and machines, the manufactured and used things themselves, and the needs and ends that they serve, all belong to what technology is. The whole complex of these contrivances is technology (Heidegger, 1977). [b]It is during this period that there first appears an abstraction of the rights independent from an object

Table I.
Progressive abstraction of intellectual property rights

2.1 Definitions

Simply speaking, trade secrets may be any business information, not generally known, that creates a competitive advantage over another business. Trade secrets are protected by federal[5], state[6] and common law. In 1939, the first Restatement of Torts was drafted and defined a trade secret as follows:

> 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 advantage over competitors who do not know or use it[7].

The Restatement (Third) of Unfair Competition, Section 39 (1995) defines trade secrets as "*any* information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others" (emphasis added).

The Economic Espionage Act (EEA) defines trade secrets as:

> . . . all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if – (a) the owner thereof has taken reasonable measures to keep such information secret; and (b) the information derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable through proper means by the public.

2.2 Purpose

The trade secret laws seek to encourage three core public policies:

(1) to maintain commercial morality because trade secret law represents an enforceable standard of business ethics allowing businesses to enter into good faith transactions, form stable business relationships, and share confidential information to gain assistance in product development;

(2) to encourage research by ensuring that innovators are the first in the market with their creations; and

(3) to punish industrial espionage by protecting the *right of privacy* of the trade secret owner (Nashieri, 2005, pp. 24-5).

Since trade secrets, in order to maintain their value, must not be revealed, how trade secret protection operates in the KM and CI world is discussed below.

3. Trade secrets, KM systems and competitive intelligence

Because KM systems require ongoing employee exchanges among colleagues and often with persons outside the organization, employees need to be made aware of what information can and should be shared[8]. In addition, Garvin (2005) suggests that to encourage employees to take part in such exchanges, they should "get something of value back in return for contributing to the system", especially if the organization wants employees not only to share, but collect additional knowledge. Competitive intelligence takes off where KM systems end[9]. Specifically, when employees cannot or do not share information about a company's business, competitive intelligence professionals use other methods to obtain critical business information[10].

Whether competitive intelligence is merely a subset of knowledge management will not be fleshed out here, but for purposes of discussion, KM as a means of leveraging an organization's strategic assets and the skills required to do so are different from competitive intelligence, which is defined by Nashieri (2005, p. 73) as a "systematic and ethical program for gathering, analyzing and managing information that can affect a company's plans, decisions, and operations". However, both have risks relating to the legitimate collection of information in a knowledge/intelligence driven economy and how it relates to trade secret rights (Simmers, 2004, p. 324):

(1) *KM risk* – what happens when a company fails to develop knowledge assets to their fullest potential – when rivals are?

(2) *CI risk* – what are the challenges a company faces in keeping knowledge assets out of competitors' hands?

How this industry and company-specific knowledge is collected, acquired, or distributed may be subject to trade secret rights enforcement.

4. Enforcement

Trade secret misappropriation relief may be sought via the criminal or civil courts. However, there is some difficulty in enforcing trade secret rights. According to Degnan and Jaros (2004, p. 4), there are three reasons why it is difficult to enforce trade secret rights:

(1) there is no longer a typical defendant;
(2) thefts are becoming harder to detect and prove; and
(3) international trade secret law is far from uniform.

The "typical defendant" of the past used to be a former employee or competitor. Nowadays, the defendant may be a hacker, a terrorist, a disgruntled current employee or an innocent internet user. Further, because a typical theft may be simply the copying of a electronic file or hard copy manifestation of the trade secret, the theft may be undetected. Finally, when the trade secret crosses national boundaries, enforcement is often difficult, if not impossible.

Japan's Ministry of Economy, Trade and Industry (METI) identified seven ways trade secrets were most commonly leaked:

(1) information was copied by employees after hours and passed on to competitors;
(2) employees worked for competitors on weekends and shared sensitive information with them[11];
(3) because local licensing laws are unknown or unenforced, trade secrets were lost when Japanese companies partnered with foreign companies[12];
(4) information was removed from foreign joint venture employees after hours;
(5) interns from a foreign company transferred information from a domestic company to their own company;
(6) there was a breach of confidentiality agreement where a company supplied protected equipment to a competitor; and
(7) reverse engineering (*Financial Times*, 2004).

A close look at these methods reveals that the leaks are often secreted by low-tech means. This implies that concentrating on internet and computer security should be only one of several ways a business should protect its trade secrets. A cursory review of the above list and EEA[13] cases indicates that employee and insider education may be severely lacking[14].

4.1 Federal protection and civil remedies

The Economic Espionage Act of 1996 represents the first time the USA has criminalized activities relating to the improper acquisition of trade secrets[15]. The Act makes it a criminal act to unlawfully acquire any trade secret for the benefit of:

- a foreign government, foreign instrumentality or foreign agent[16]; or
- anyone other than the owner of the trade secret[17].

The criminalization of trade secret misappropriation represents an acknowledgement by the US Government that its domestic businesses are under economic attack[18]. According to a PriceWaterhouse publication, *Trends in Proprietary Information Loss*, "70 percent or more of the market value of a typical U.S. company may derive from its intellectual property (IP) assets"[19]. Apparently, civil remedies, which include injunctions and monetary damages, are not enough. Indeed, many businesses consider the enforcement of such legal remedies merely the cost of doing business[20]. In

addition, those businesses who have been victims of trade secret theft are reluctant to disclose the any breaches for fear of shareholder retaliation or loss of market share[21].

According to Nashieri (2005), while potential defendants may ignore trade secret civil claims because the damages may be included in the cost of doing business, criminal liability may help with general deterrence because the government is treating trade secrets much like any other personal or real property[22]. One downside to criminalizing trade secret misappropriation is that the EEA could become a litigation tool because "virtually any infringement could be criminalized and a vindictive litigant could refer a case to prosecutors as a competitive tool or litigation strategy" (Nashieri, 2005, p. 177).

5. Scenario

Having discussed the laws and issues relating to trade secrets, I would like to set up the scenario under which I will answer my student's question, i.e.. if a business supplies information that otherwise is in the public domain, would that business be liable due to its revealing of trade secret information?

5.1 Presumptions

I will presume the following:

- Private Entity A is under contract with the US Government to provide services the Government would otherwise have to do itself, but for economic, expertise or other resource issues, the Government chooses to contract these services out to the private sector;
- the Government's purposes for contracting out these services are legal;
- Private Entity A provides commercial remote sensing space system services to the US ates Government and is under license to do so;
- Private Entity B, a separate US-based private business, has discovered that trade secret information has been made available to competitors from Private Entity A and was not informed of the possibility that it would be subject to remote sensing surveillance;
- Private Entity B has made reasonable efforts to maintain and protect its trade secrets; and
- Private Entity B has suffered damages and is considering both civil and criminal remedies.

5.2 Federal law

Under the EEA, the lawful activities of a government entity are not prohibited[23]. In the event that a party has participated in activity subject to EEA scrutiny, a federal prosecutor must prove beyond a reasonable doubt that the defendant:

- acted with specific intent to convert the trade secret with the knowledge that the trade secret was proprietary or closely guarded;
- attempted to or conspired to convert the trade secret for the economic benefit of anyone other than the rightful owner; and
- intended or knew that the conversion offense would injure the lawful owner of the trade secret[24].

Any person found guilty under EEA is subject to a fine or imprisonment. A business may be fined not more than $5 million[25].

5.2.1 Federal law – licensing. The General Conditions for private remote sensing space system licenses require that the licensee "shall comply with [...] any and all applicable laws, and any applicable regulations issued pursuant to the Land Remote Sensing Policy Act of 1992 ('the Act')". The President authorized a new national policy on US commercial remote sensing on April 25, 2003. This new policy states that its goal is "to advance and protect U.S. national security and foreign policy interests by *maintaining the nation's leadership in remote sensing space activities, and by sustaining and enhancing the U.S. remote sensing industry*" (emphasis added). In addition, the US Government will rely "to the maximum practical extent on U.S. commercial remote sensing space capabilities for filling imagery and geospatial needs for military, intelligence, foreign policy, homeland security, and *civil users*" (emphasis added). Moreover, a robust US commercial remote sensing space industry "can augment and potentially replace some United States Government capabilities and can contribute to U.S. military, intelligence, foreign policy, homeland security, and civil objectives, as well as *U.S. economic competitiveness*" (emphasis added). Finally, "because of the potential value of its products to an adversary, the operation of a U.S. commercial remote sensing space system requires appropriate security measures to address U.S. national security and foreign policy concerns"[26].

5.3 Common law – liability

To establish whether something is a trade secret, a potential plaintiff must show that the information is a secret and that it was improperly acquired or disclosed. In order to succeed on a trade secret misappropriation claim, the plaintiff must also show that the defendant breached a confidence or acquired the trade secret by improper means. The remedies a plaintiff may seek include an injunction as well as actual and punitive damages. Traditionally, for an appropriation of trade secrets to be wrongful the party must have:

- trespassed;
- committed some other illegal conduct, including improper means; or
- breached a confidential relationship[27].

5.3.1 Common law – trespass and privacy. A privacy claim is a variation on a trespass to property claim. Similar legal analysis applies. If someone enters onto another's land without a license or some other claim of right (such as retrieving one's property or to prevent an injury), that person has trespassed. If someone enters into the "zone of privacy" of another, that person has "trespassed" on that person's privacy rights.

For an aerial trespass claim to succeed, the plaintiff must show that there was an interference with an existing use or that there was an imminent danger to persons or property and the altitude at which the surveillance machine was flying was low.

Privacy protection is obviously ephemeral, but generally, a person has a cause of action if a defendant conducts unwarranted searches, eavesdrops, conducts illegal surveillance, appropriates one's identity, or appropriates and misuses one's communications (*Stanford Encyclopedia of Philosophy*, 2002).

5.3.2 Common law – improper means. *E.I. duPont deNemours & Co., Inc.* v. *Rolfe Christopher, et al.*[28], for the purposes of this section, is the common law standard to review whether the activity a commercial remote sensing business may be subject to civil liability for trade secret misappropriation.

Briefly, the defendants in this case argued that they committed no "actionable wrong" photographing the duPont facility because they (p. 1014):

- conducted their activity in public airspace;
- violated no government aviation standard;
- did not breach any confidential relationship; and
- conducted no fraudulent or illegal conduct.

Having found that the parties did not breach a confidential relationship, nor did they trespass, the court determined that the "question remaining, therefore, is whether aerial photography of plant construction is an improper means of obtaining another's trade secret" (p. 1015). In this instance, the court found that aerial photography of plant construction was an improper means of obtaining another's trade secret.

5.3.2.1 Common law – improper means – direct and vicarious liability. If a system, or in this case, a remote sensing device, merely stores, receives and makes images available, without knowledge as to the ultimate user's use or purpose for the images, its operators may not be found liable for direct misappropriation if one applies copyright direct liability standards. However, vicarious liability may be found.

Although there are no express provisions for vicarious liability under USTA or EEA, it is useful to look at similar provisions in copyright vicarious liability cases[29]. Vicarious liability for improper activities may be found if a defendant:

- is responsible for supervising activity that may constitute an intellectual property infringement; and
- enjoys a direct financial interest in this activity (*Fonovisa, Inc.* v. *Cherry Auction, Inc.*, 76 F.3d 259, 2642 (9th Cir. 1996)).

If a company has the right and ability to control, or supervise, a "system's premises", it is, therefore, responsible to ensure that the material contained on it is not used for illegal purposes (*A&M Records* v. *Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001)). In addition, financial benefit "exists where the availability of the infringing material 'acts as a 'draw' for customers" (*Fonovisa*, 76 F.3d at 363-64).

In *Tao of Systems Integration, Inc.* v. *Analytical Services & Materials, Inc.*, 299 F.Supp. 2d 565, 575 (E.D. Va. 2004), the court found that "[a]n employer can be held vicariously liable for trade secret misappropriation committed by an employee within the scope of his employment".

Under Virginia Uniform Trade Secret Act, which applied in the above case, acts that may constitute misappropriation include:

> [D]isclosure or use of a trade secret without consent by a person who, at the time of disclosure or use *knew* or *had reason to know* that his knowledge of the trade secret was either
>
> (1) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(2) Derived from or through a person who owed a duty to maintain its secrecy or limit its use (*Tao*, at 575 and Va. Code Ann. § 59.1-336; emphasis added).

5.4 Public domain

Once a trade secret is made available to the public, or becomes generally known, it loses its trade secret status and enters into the public domain. However:

> . . . [t]he means by which the discovery is made may be obvious, and the experimentation leading from known factors to presently unknown results may be simple and lying in the public domain. But these facts do not destroy the value of the discovery and will not advantage a competitor who by unfair means obtains the knowledge without paying the price expended by the discoverer (*Brown* v. *Fowler*, 316 S.W. 2d 111, 114 (1958)).

6. Analysis

So what result for our hopeful plaintiff (Private Entity B)? Perhaps the best tactic the plaintiff can start off with is an appeal to the government's public policy position. If the plaintiff chooses the EEA route, the plaintiff may have difficulty meeting the "proof beyond a reasonable doubt" standard as to the three elements. However, because the federal government has a special interest in securing the economic well-being of the country, as well as securing its own national security interest, a federal prosecutor may be willing to go forward with such a case.

In addition, the federal prosecutor may be able to show that the putative defendant (Private Entity A) breached its licensing agreement with the government if it could be found that the defendant did not comply with all applicable laws (including trade secret laws) as required.

If the plaintiff decides to pursue its claims civilly, trespass and breach of confidential relationship claims are not likely to succeed. Satellites, if operating properly, do not orbit low to the ground and the hypothetical scenario does not involve a confidential relationship.

Like the *duPont* case[30], the plaintiff's best bet may be to argue that although the images were allegedly in the public domain, the means by which the trade secrets were misappropriated were unfair and the defendant's acquisition and use of them would confer upon the defendant a economic windfall because that business did not have to pay the expense of discovering, developing and protecting the trade secret[31]. In addition, the activity infringed upon the plaintiff's commercial privacy. Indeed, the most successful argument here may be that made Judge Goldberg:

> Our tolerance of the espionage game must cease when the protections required to prevent another's spying costs so much that the spirit of inventiveness is dampened. Commercial privacy must be protected from espionage which could not have been reasonably anticipated or prevented. We do not mean to imply, however, that everything not in plain view is within the protected vale, nor that all information obtained through every extra optical extension is forbidden [. . .] Perhaps ordinary fences and roofs must be built to shut out incursive eyes, but we need not require the discoverer of a trade secret to guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available (*duPont*, at 1016).

The plaintiff is still not out of the woods because "[r]emedies become complicated, since a plaintiff – even after becoming aware of the existence of some surveillance –

may lack full knowledge of the complete extent of the surveillance, leading to evidentiary problems" (Friedman, 2003, p. 40).

The next best cause of action may be set forth under vicarious liability theory, e.g. even though the defendant is providing a legal service, a court or jury may find that its activities would fall within the two-pronged vicarious liability standard. Specifically, the defendant may be found responsible for supervising activity that may constitute an intellectual property infringement and that it enjoys a direct financial interest in this activity.

Will our plaintiff succeed? There appears to be an unintended and untested policy conflict. On one hand, the US Government has given itself a powerful tool to protect trade secrets held dear by its companies and the nation[32]. On the other, the US Government has granted licenses to commercial remote satellite companies which may, inadvertently, sell satellite images to industrial competitors, consequently thwarting trade secret protection efforts. So the answer is . . . maybe.

This area of the law may never be resolved, for many of the reasons discussed in this article, including hesitancy of companies to come forward with trade secret theft allegations, as well as the more likely reason that most companies are not aware that their trade secrets have, in fact, been revealed via commercial satellite surveillance.

7. Conclusion

Competitive intelligence itself is not illegal. Companies who fail to conduct some sort of competitive intelligence within their industries will lose market advantage. However, entities that wish to protect the business proprietary information they have should ensure that adequate measures are taken to protect that information from being disclosed. The question remains what constitutes "adequate" or "reasonable" protection means when satellite surveillance is involved.

Anyone who acquires trade secret information via improper means is subject to the consequences[33]. Trade secret protection will not be accomplished simply by banning the movement of individuals to different countries or companies or prohibiting certain types of technology. Innovative companies take the risk that their knowledge will and does walk out. Their best defensive strategies a knowledge-intensive company can implement include:

- educating employees;
- enforcing existing trade secret and confidential information policies;
- properly identifying trade secret and confidential information; and
- not only making "reasonable" efforts to protect trade secrets, but to aggressively monitor whether their efforts are keeping up with technological and industry standards[34].

Notes

1. The technology is remarkable. Unless you live in a remote corner of the world or your address is not tracked, anyone can find your home (see http://nationalmap.gov).
2. In the USA, copyrights are generally protected for the life of the author plus 70 years. Patents are protected for 20 years.

3. Note, however, that if the trade secret itself is a legal dispute's core issue, and deemed relevant and essential to resolve that issue (for example, whether Diet Coke and Coca-Cola are the same product), the court may require that the secret be divulged, despite the court's acknowledgement that the trade secrets are subject to the maximum protection the law allows. See, *Coca-Cola Bottling Company of Shreveport, Inc.* v. *The Coca-Cola Company*, 107 FRD 288 (D. Del. 1985).
4. "[T]he question is not whether there should be a property interest or some form of ownership in the fruits of one's intellectual labor, but rather the question is how powerful should that property interest be since there is a countervailing societal interest in the dissemination of knowledge for the benefit of all" (Nashieri, 2005, p. 181).
5. Economic Espionage Act of 1996, Title 18, United States Code, Chapter 90.
6. Forty-five states and the District of Columbia have modeled trade secret statutes after the Uniform Trade Secrets Act. Generally, the following factors may be considered to determine whether something is a trade secret: "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy" (USTA, with 1985 amendments).
7. Restatement of Torts, §757, Comment b (1939).
8. For a useful and informative discussion on the relationship between competitive intelligence and knowledge management, see Parker and Nitse (2005).
9. Increasingly, businesses are moving from "hierarchical bureaucratic organizational forms": toward a "new" organizational form that is "sensitive to vertical, horizontal, and external challenges and opportunities". This "new form" of organization differs from the hierarchical organization and "recognizes that exchanges outside the organization [. . .] are critical to organizational survival and growth" (Simmers, 2004, p. 228). Nashieri (2005, p. 73) suggests that competitive intelligence consists of two steps. First, the CI professional uses public sources to develop data on competition, competitors and the market environment. Second, the CI professional transforms that data into information which will support business decisions.
10. For the purposes of clarity, "competitive intelligence" will be distinguished from "corporate espionage", which involves the theft of proprietary information. The line between the two is addressed in the "Scenario" section.
11. "Former employees continue to represent the highest risk factor in the loss of trade secrets" (Degnan and Jaros, 2004, p. 3).
12. This dilemma will only become more problematic in the future because "[c]ompanies around the world are increasingly forced to share critical proprietary information with customers, suppliers, contractors, consultants, and strategic partiers during the early stages of product development" (Nashieri, 2005, p. 50).
13. Of the 33 prosecuted cases under EEA, 14 were former employees, two were competitors, 12 were insiders, and five were outsiders (see www.cybercrime.gov/eeapub.htm). Two press releases issued by the Justice Department in February 2007 involved trade secret theft by employees (see www.cybercrime.gov/grandePlea.htm and www.cybercrime.gov/chilowitzPlea.pdf).
14. While I have argued for less restrictive employee mobility under non-competition and non-disclosure provisions in employee agreements, I do not think that educating employees about trade secret protection is contrary to this position (see Gayton, 2006). See also Nashieri (2005, p. 177): "One cost of enhanced rights in trade secrets is that exercising those rights

impedes the ability of employees to take jobs in other firms or to start new businesses. Loss of employee mobility leads to another cost, or inefficiency, by affecting regional economic performance". But consider General Assembly Resolution 217A (III), UN Doc. A/810, at 71 (1948): Article 19. "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers".

15. "EEA is the first federal law in the United States designed to protect trade secrets" (Nashieri, 2005, p. 129). Despite initial high hopes for prosecution under EEA, only 33 cases have been successfully prosecuted as of 2005 (see www.usdoj.gov/criminal/cybercrime/eeapub.htm; accessed March 18, 2007).
16. Sec. 1831. Economic Espionage.
17. Sec. 1832. Theft of trade secrets.
"(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly–
(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
(4) attempts to commit any offense described in paragraphs (1) through (3); or
(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.
(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000".
18. "A nation's economic status makes up a large part of its national security. This economic status is dependent on a nation's ability to compete efficiently in the world market" (Nashieri, 2005, p. 2).
19. Notably, the report indicates that "formalized valuation procedures exist in too few companies to assure that managements have a complete appreciation of the extent and importance of these resources" (Nashieri, 2005, p. 3).
20. See *Advanced Marine* v. *PRC*, 256 Va. 106, 501 S.E. 2d 18 (1998) where appellant, Advanced Marine, knew that the engineering team personnel it was recruiting had signed non-compete agreements. Despite the threat of being sued for tortuous interference with contract, Advanced Marine hired the engineers anyway.
21. "For many companies, security and control over their operations and assets are vital to their success, and thus reporting breaches in that security is potentially damaging to future business [...] Companies are also reluctant to report [...] thefts because they can spawn unwanted attention from the Securities and Exchange Commission and shareholder derivative suits. Probably the greatest reason why trade secret theft is not prosecuted more often is the failure of victims to report such thefts to government authorities. Companies are reluctant to report such crimes because of concern over a loss of public trust and public image" (Nashieri, 2005, p. 52).
22. But see, Ben-Atar (1004, pp. 4-5): "Natural rights association of intellectual and physical property is problematic. First, physical property is inherently a zero-sum game which

knowledge is not. An owner of an ax loses his ability to use it when it is stolen. An inventor, however, can still use his invention even when others duplicate it. The inventor is the loss of exclusivity that undermines his potential profit margin [. . .] Second, physical property does not cease to exist in law through time while intellectual property, in the form of either patent or copyright, is always confined to a specific number of years. Finally, the natural rights perspective runs counter to the interests of the state, for it locates the value of an innovation in the creative individual and contends that intellectual property is not confined by international boundaries".

23. Sec. 1833. Exceptions to prohibitions
This chapter does not prohibit–
(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or
(2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

24. Derived from Seltzer and Burns (1999).

25. 18 USC § 1832.

26. See www.licensing.noaa.gov/eolicense.htm. But see also: "[t]echnical innovation provides new ways to resolve international problems, but also creates new foreign policy headaches. For example, satellite surveillance can help verify compliance with arms control treaties, but the commercial market in high resolution imagery and global positioning data also can provide rogue nation or terrorist groups with critical intelligence" (Nashieri, 2005, p. 36).

27. Because there is not likely a breach of a confidential relationship in my scenario, it will not be addressed.

28. 431 F.2d 1012 (5th Cir. 1970).

29. "For vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another" (*Sony Corp.* v. *Universal City Studios, Inc.*, 464 U.S. 417, 435, 78 L. Ed. 2d 574, 104 S. Ct. 774 (1984)).

30. DeSassure (1977, p. 711) determined that aerial surveillance similar to remote sensing in several ways: (1) each provides an overhead view of the subject, the earth; (2) each can penetrate every corner of the globe without the normal obstructions and hazards of earthbound vehicles and vessels; (3) each can perform repetitive, and in varying degrees, syntopic coverage of the earth's surface. Although DeSassure's article was published in 1977, important legal issues remain for purposes of my analysis: "Is the data generated by remote sensing satellite or the information derived from this data subject to individual proprietary rights?". These individual proprietary rights may include privacy rights. DeSassure found that the *DuPont* decision was significant to remote sensing in two ways: (1) there still could be a tort even though there was no trespass; and (2) the parties were not those who used or wanted the information – rather, they were hired by others.

31. "The observer gains value. The use of information gained from visual aerial surveillance for purely commercial means, such as market research, is more *economically* troublesome as an unfair appropriation of value than would be the use of information for academic study, or to uncover facts related to legal disputes or other wrongdoing [. . .] But even information that is not directly used in business would still confer upon the observer economic value that was obtained from [. . .] a non-public location" (Friedman, 2003, p. 15).

33. A nation's economic status makes up a large party of its national security. This economic status is dependent on a nation's ability to compete efficiently in the world market" (Nashieri, 2005, p. 2).
33. Sometimes, the money is enough. "Those who develop a competitive advantage over their rivals stand to make millions from their innovations. That profit is enough for some to seek an unwarranted advantage of their own by indulging in corporate espionage as a quick-fix solution to their creative deficiencies and their inability to remain competitive in their field" (Nashieri, 2005, p. 54).
34. Courts only require "reasonable efforts" to maintain the secrecy of the information. Even with security measures, should ensure that these measures are up to date (Degnan and Jaros, 2004, pp. 6-7). "While the cost of defending a trade secret against emerging technology may continue to increase, one point remains: *the value of a trade secret is measured by the extent of the efforts used to protect it*" (Degnan and Jaros, 2004, p. 18).

References

Ben-Atar, D.S. (2004), *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*, Yale University Press, New Haven, CT.

DeSassure, H. (1977), "Remote sensing by satellite: what future for an international regime?", *American Journal of International Law*, Vol. 71 No. 4, pp. 703-24.

Degnan, D. and Jaros, J. (2004), "The present value of trade secret protection: do the costs outweigh the benefits?", Holland & Hart LLP, available at: www.iph2.com/AIPLA.pdf (accessed March 16, 2007).

Financial Times (2004), "The seven routes for trade secrets to leak out", *Financial Times*, February 9, available at: www.ft.com (accessed March 18, 2007).

Friedman, J. (2003), "Prying eyes in the sky: visual aerial surveillance of private residences as a tort", *Columbia Science and Technology Law Review*, Vol. 4.

Garvin, J. (2005), "Ethics of intelligence: keeping your hands clean", *From Knowledge to Intelligence*, Elsevier Butterworth-Heinemann, Burlington, MA, pp. 303-22.

Gayton, C. (2006), "Legal issues for the knowledge economy in the twenty-first century", *VINE*, Vol. 36 No. 1, pp. 17-26.

Heidegger, M. (1977), *The Question concerning Technology* (trans. by Lovitt, W.), Harper Torch Books, New York, NY.

Nashieri, H. (2005), *Economic Espionage and Industrial Spying*, Cambridge University Press, Cambridge.

Parker, K.R. and Nitse, P.S. (2005), "Improving competitive intelligence for knowledge management systems", *International Journal of Internet and Enterprise Management*, Vol. 3 No. 1, pp. 24-45.

Seltzer, M. and Burns, A. (1999), "Criminal consequences of trade secret misappropriation", *B.C. Intell. Prop. & Tech.*, 052501, May 25, available at: www.bc.edu/bc_org/avp/law/st_org/iptf/articles/content/199052591.html (accessed March 15, 2007).

Simmers, C. (2004), "A stakeholder model of business intelligence", *Business Intelligence Techniques*, pp. 227-42.

Stanford Encyclopedia of Philosophy (2002), "Privacy", available at: http://plato.stanford.edu/entries/privacy (accessed June 29, 2006).

Further reading

Anadarajan, M., Arandarajan, A. and Srinivasan, C. (Eds) (2004), *Business Intelligence Techniques*, Springer-Verlag, Berlin.

Dutka, A. (1999), *Competitive Intelligence for the Competitive Edge*, NTC Business Books, Chicago, IL.

Rothberg, H. and Erickson, G.S. (2005), *From Knowledge to Intelligence*, Elsevier Butterworth-Heinemann, Burlington, MA.

WIPO Magazine (2002a), "Trade secrets are gold nuggets: protect them", April, available at: www.wipo.int/sme/en/documents/wipo_magazine/04_2002.pdf (accessed March 8, 2007).

WIPO Magazine (2002b), "Trade secrets: policy framework and best practices", May, available at: www.wipo.int/sme/en/documents/wipo_magazine/05_2002.pdf (accessed March 8, 2007).

About the author

Cynthia M. Gayton holds a Bachelor of Arts degree in International Affairs from The George Washington University and a Juris Doctor degree from George Mason University in Arlington. Cynthia is a member of both the State Bar of Virginia and the District of Columbia Bar. Before joining the AIA, Cynthia had her own practice specializing in intellectual property and corporate law. In addition, she worked as an attorney at Morgan Lewis & Bockius, concentrating in complex antitrust litigation. Additionally, Cynthia is a part time adjunct professor of engineering law at The George Washington University School of Engineering and Applied Sciences. Cynthia is the co-author of *Legal Aspects of Engineering*, released in August of 2004 by Kendall/Hunt publishers, and "Knowledge management in the large law firm" (available at www.knowledgeboard.com). Cynthia Gayton can be contacted at cgayton@gwu.edu