The Economic Espionage Act: The Rules Have Not Changed

Richard Horowitz, Esq.

Legal and Investigative Services

EXECUTIVE SUMMARY

The author argues that the Economic Espionage Act of 1996 was never intended to limit aggressive but legitimate competitive intelligence collection activities, nor even activities that fall into the "gray zone," and that CI professionals who are properly trained and abide by SCIP's Code of Ethics should not run afoul of trade secret law or the EEA. The clearly criminal activities the EEA targets have always been prohibited under state law and unacceptable under SCIP's Code of Ethics. Moreover, trade secret case law has interpreted "misrepresentation" as applying to situations which induce a breach of confidentiality. Using "pretexts" to elicit information may be unethical, but isn't illegal under most circumstances. © 1998 John Wiley & Sons, Inc.

The effect of the Economic Espionage Act (EEA) on competitive intelligence has become a matter of concern among many CI practitioners and firms since its enactment in October 1996. I took an active interest in this issue because of a comment made at SCIP's February 1997 EEA Symposium. During a break after the panel of lawyers, I heard one attendee ask his colleague if they now could be subject to an FBI arrest by attending a trade show without a company name on their name tag because the EEA prohibits misrepresentation.

I spoke the following day and stated that the EEA was not intended to regulate the CI community nor was it developed in response to any problems arising from the CI community; that the EEA does not change the rules of game—only the consequences of violating them, and that my concern was not that the Department of Justice would misuse this law but that companies and their attorneys might attempt to use the EEA to intimidate their competitors who are attempting to collect competitive intelligence on them.

Since then I have come across numerous situations where CI professionals have been under pressure from their companies to curtail their activities, others who have had to endure the anxiety that their jobs may be

Competitive Intelligence Review, Vol. 9(3) 30–38 (1998)
 CCC 1058-0247/98/03030-09

eliminated for fear of legal liability, and still others who are hesitant to proceed with their work, either because they are unsure of what the EEA means or what action others may take against them because of the EEA.

The peculiar irony of this situation is that CI practitioners who are properly trained and abide by SCIP's Code of Ethics should not run afoul of trade secret law or the EEA. This is because the appropriate legal standards have been instilled in the CI profession in the decade that SCIP has been in existence. Again, from personal experience I know many CI professionals who "are doing everything right" from a legal perspective but cannot explain why this is so in legal terms.

APPROPRIATE LEGAL STANDARDS HAVE BEEN INSTILLED IN THE CI PROFESSION IN THE DECADE THAT SCIP HAS BEEN IN EXISTENCE.

The key to understanding why the EEA is fundamentally irrelevant to CI that is conducted consistently with SCIP's Code of Ethics is to recognize that trade secret law is not new. For decades, one who misappropriated a competitor's trade secrets was subject to civil liability under state law and, in some states, criminal liability. Trade secret cases from the 19th century are still quoted in court today.

Being charged with the responsibility of protecting national security and the national economy, and, confronted with the reality that laws dealing with the theft of trade secrets were state law, federal authorities needed a federal statute to give them the authority to investigate and prosecute the increasing number of cases of economic espionage conducted by foreign entities.

The EEA was enacted to enable federal authorities to do just that.

Congress decided, however, that the scope of the EEA would include the theft of a trade secret by anyone, for anyone. In other words, the EEA is not limited to theft of a trade secret for a foreign entity, but encompasses theft of a trade secret by and for a domestic competitor.[a]

[a]Peter Toren, the Justice Department official most closely associated with the EEA, co-authored an article which contained the following: "Originally, the bill applied only to thefts of trade secrets that were intended to benefit a 'foreign government, foreign instrumentality, or foreign agent.' Concerns that such a law might violate a number of international trade treaties to which the United States is a signatory caused the bill to be rewritten at the last minute to include both foreign and domestic theft of trade secrets." ("EEA Violations Could Trigger Criminal Sanctions," by Hoken S. Seki and Peter J. Toren, *The National Law Journal*, August 25, 1997).

Herein lies the confusion. While the EEA makes trade secret law a federal criminal matter—this for the first time in U.S. history—the activities it criminalizes were prohibited under state law and/or unacceptable under SCIP's Code of Ethics. In other words, the rules are fundamentally the same, but the consequences of violating them are different. An activity that had always been a violation of state trade secret law can now result in not only state civil liability but federal criminal liability as well.

Adding to the confusion regarding the EEA has been a series of articles and presentations that has created the impression that the EEA fundamentally alters how CI professionals must conduct their affairs: "New Spy Law Could Cramp Economy,"[1] "New Spy Act To Boost White-Collar Defense Biz,"[2] "Go Directly To Jail: New Federal Law Protects Trade Secrets,"[3] "U.S. Economic Espionage Act: Tough EEA Enforcement Reveals Need for Strict Compliance,"[4] "The Economic Espionage Act: A Wake-Up Call,"[5] "The Economic Espionage Act: Turning Fear Into Compliance,"[6] "Economic Espionage Act: A Whole New Ball Game."[7] Among the more notable assertions:

> *"Your industry is crawling with criminals. And you may be one of them. So might your company . . . Cases involving a customer list used to be a concern only of private lawyers; now they can be investigated by the FBI and prosecuted by the Department of Justice. All of this came about with the enactment of the [EEA] . . . the fact of its passage will surely lead to greater interest in federal jurisdiction over civil trade secret disputes."*[8]

> *"The risks of a federal offense are high and the consequences costly and severe."*[9]

> *"The [EEA] makes theft of trade secrets a federal crime with stiff penalties of up to $10 million and 15 years in prison for violations. Under current standards of business practice, a sales representative, vendor, consultant, market researcher, or curious employee could subject an organization to an FBI raid and investigation leading to federal prosecution."*[10]

The first wave of pro-EEA material argued that there exists "a new list of activities" prohibited by the EEA that CI professionals must avoid. Unable to articulate what these activities are, the pro-EEA proponents now speak of a changed "risk management equation," that risks CI practitioners might have taken in the past have become untenable with the passage of the EEA.

An understanding of trade secret law and our legal system is necessary to recognize whether these assertions have merit.

That the legal consequences facing one who steals a trade secret are far more severe under the EEA does not mean that these consequences prior to its passage were not serious. It is inconceivable that responsible corporate counsel or outside attorneys would not dissuade their companies or clients from engaging in legally risky behavior if the potential sanctions were "only" state civil as opposed to federal criminal. Moreover, after much research including conversations with numerous CI industry veterans, pre-EEA litigation involving CI professionals who misappropriated trade secrets is apparently non-existent. As a criminal statute, EEA cases require a higher burden of proof than state trade secret cases, which in part explains why EEA charges filed to date have implicated clear-cut criminal activity.[b] That "gray zone" activity that has in fact taken place among CI professionals did not generate state trade secret litigation indicates that the risks of the EEA being implicated in these situations is low indeed.

EEA CHARGES HAVE ONLY IMPLICATED CLEAR-CUT CRIMINAL ACTIVITY. THE RISKS OF THE EEA BEING IMPLICATED IN "GRAY ZONE" SITUATIONS IS LOW INDEED.

Another reason why the risk of the EEA being associated with routine commercial disputes is low can be found in the article co-authored by Mr. Toren,[11] where he wrote that the act of a U.S. citizen anywhere could violate the EEA: "This conceivably means that if a U.S. citizen residing abroad steals a Russian trade secret on behalf of the Chinese government, that act violates the EEA . . . Congress, however, likely did not intend to reach situations in which the United States does not have a legitimate national interest."

What comes to my mind is a case I learned in law school: Driver is sober, passenger drunk. Driver parks and exits the car, which begins to roll down the hill. Though drunk, passenger moves into the driver's seat, turns the steering wheel to avoid hitting a tree and applies the brakes. Police arrest passenger for being "in control of a motor vehicle" while in a state of intoxication.

Though surely beyond intention of the legislature, a strict reading of the statute would apply it to the facts of this case. Is it, however, a correct application of the law?

To insure that the EEA will not be applied to situations inconsistent with Congressional intent for the law, Attorney General Janet Reno promised Congress that no charges will be brought under the EEA for the first five years without the authorization of the Attorney General or two of her top deputies.[12]

In other words, to maintain that the EEA will be applied to commercial "gray zone" cases, one must believe, in light of General Reno's letter, that the *very top* Justice Department decision-makers would, first, take an interest in the case and, second, file a criminal charge where they could not be confident of a victory in civil court, in situations not intended to be covered by Congress.

"Gray Zone" Activities

The most significant reason, however, why the EEA should not be of concern to CI professionals who abide by the industry's standards of ethics is that many situations which have come to be known as "gray zone" activities are not really trade secret violations at all. Finding a lost document in the street, overhearing competitors talk on a plane, having a drink with a competitor knowing you are better at holding your liquor, removing your name tag at a trade show, or even falsely identifying yourself as a student, are situations that alone will not trigger trade secret liability. As I wrote in the beginning of this article, the appropriate legal principles have been instilled into the CI profession over the years and the many "gray zone" sessions sponsored by SCIP attest to this: attendees can generally (1) recognize what activities are clearly illegal, and (2) understand when to rely on their ethical instincts with respect to "gray zone" issues.

A short analysis of trade secret law as it applies to competitive intelligence is in order. Note, that the following is intended to explain the fundamentals of trade secret law and not to answer legal questions that may arise.

[b]Often in civil trade secret litigation, the issue essential to the case such as (1) Is the information in question a trade secret?, (2) Were reasonable measures used to keep the information secret?, (3) Were the means of acquiring the information improper?, are questions to be answered by the jury. In a criminal case, the prosecutor would want to be certain that the basic elements of the crime can be established as easily as possible rather than rely on jury deliberations. This supports the contention that EEA cases will be based on clear-cut criminal activity such as bribery and clearly recognizable trade secrets such as chemical formulas or blueprints. The five EEA cases to date support this. For a summary of these cases, see "In the Spotlight: Four Cases Under the EEA," *The Corporate Counselor,* November, 1997, and *U.S. v. Kai-Lo, U.S. v. Ho,* FBI Charges Tawainese Tried To Steal Taxol Trade Secrets from BMS, *Intellectual Property Litigation Reporter,* June 18, 1998.

A paragraph from the Restatement of Torts (1939)[c] which surprisingly I have not found cited in any published material on CI, points to the legal validity of competitive intelligence:

> *The privilege to compete with others includes a privilege to adopt their business methods, ideas, or processes of manufacture. Were it otherwise, the first person in the field with a new process or idea would have a monopoly which would tend to prevent competition.*[13]

One limitation on this rule cited by the Restatement is:[d]

> *when the thing copied is a trade secret . . . The significant difference of fact between trade secrets and the processes or devices which are not secret is that knowledge of the latter is available to the copier without the use of improper means to procure it, while knowledge of the former is ordinarily available to him only by the use of such means. It is the employment of improper means to procure the trade secret, rather than the mere copying or use, which is the basis of liability in this section.*

Consider the following general points with respect to the applicability of trade secret law to competitive intelligence.

1. *Trade secret law protects the holder of a trade secret from someone who "misappropriates" that trade secret—i.e., obtains that trade secret through "improper means."*
2. *Trade secret law does not protect the trade secret information itself. In other words, a trade secret is not a patent. It is legal to "figure out" another's trade secret if all the collection methods used to acquire the information were themselves legal.*
3. *Trade secret law considers misrepresentation an improper mean.*
4. *Case law has interpreted misrepresentation to apply to situations where:*
   a. *One has induced another to violate his duty of confidentiality to his employer.*
   b. *One has violated a confidential relationship with another.*
   c. *One has acquired a trade secret from another knowing that the other had misappropriated the trade secret or that he had violated his duty to keep the information secret.*

Misrepresentation and Pretexts

How then are these principles applied to the numerous "gray zone" situations that may confront a CI professional? Has one broken the law by identifying himself to a competitor as a student?

Focusing on pretext situations, the first reason that most "gray zone" activities are not trade secret violations is because rarely does a question produce a trade secret. That a competitor would not have spoken to you had he known your real identity does not mean that what he told you was a trade secret.

THAT COMPETITORS WOULD NOT HAVE SPOKEN TO YOU HAD THEY KNOWN YOUR REAL IDENTITY DOES NOT MEAN THAT WHAT THEY TOLD YOU WAS A TRADE SECRET. THAT A COMPANY CONSIDERS CERTAIN INFORMATION CONFIDENTIAL DOES NOT ALONE MAKE IT A TRADE SECRET.

That a company considers certain information confidential does not alone make that information a trade secret. Most importantly, violating trade secret law requires that the *misrepresentation induce a breach of confidentiality.* A question that elicits an answer is not an inducement. Consider that a trade secret holder is under a duty to keep that information confidential; therefore whatever information he stated which did not encompass a violation of that duty would not be trade secret information. The competitor may very well have answered the question had the questioner truly been a student; that the questioner misrepresented himself does not mean it was the misrepresentation that induced the answer. Rather, the question itself, irrespective of the identity of the questioner, elicited an answer.

Trade secret law does not regulate the level of honesty one displays in interpersonal or even in business relations. That is the contribution of ethics. This issue of course is most provided CI professionals abide by SCIP's Code of Ethics, which expects CI professionals to accurately disclose their identity prior to all interviews. What about disclosing your identity but not your motives? One is not under a legal duty to disclose his motive or purpose.

[c]A Restatement is itself not law. *Black's Law Dictionary* defines the Restatement as follows: "A series of volumes authored by the American Law Institute that tell what the law in a general area is, how it is changing, and what direction the authors (who are leading legal scholars in each field covered) think this change should take. . . The various Restatements have been a formidable force in shaping the disciplines of the law covered; they are frequently cited by courts and either followed or distinguished; they represent the fruit of the labor of the best legal minds in the diverse fields of law covered" (p. 1313, Sixth Edition, 1990).

[d]The two other limitations cited are (1) when the information is patented, and (2) "copying in a manner which creates in the market avoidable confusion of commercial source. The privilege to copy is not a privilege to palm off one's goods as those of another."

THERE IS NO LEGAL DUTY TO DISCLOSE MOTIVE OR PURPOSE TO A COMPETITOR WHEN ELICITING INFORMATION.

To be precise, what a trade secret means is that the law will protect that information from someone who uses improper means to acquire it. Consequently, acquiring the trade secret through legal methods does not result in a trade secret violation. Furthermore, the trade secret holder will forfeit trade secret protection if the measures taken to keep the information secret were not reasonable.

One case in point: *A* decides to sell its tangible assets but not its intellectual property. *A* sells a computer to *B* but neglects to erase its customer list from the computer's memory. After the sale, *B* visits *A*'s premises to see the computer and hires *A*'s former employee to demonstrate its use, who then prints *A*'s customer list for *B*. Did *B* misappropriate *A*'s trade secret? According to a federal court in New York, *B* did not:

> *"A customer list developed by a business through substantial effort and kept in confidence may be treated as a trade secret and protected at the owner's instance against disclosure to a competitor, provided the information it contains is not readily available . . . However, the owner is entitled to such protection only as long as he maintains the list in secrecy; upon disclosure, even if inadvertent or accidental, the information ceases to be a trade secret and will no longer be protected . . . Hence even though [defendant] may have obtained the lists by improper means paying—a former employee of [plaintiff] to extract the information from the computer—any such impropriety does not create liability for use of a trade secret, since by failing to protect the lists from ready access by [defendant] independently of [the former employee's] assistance, [plaintiff] had forfeited the protections of trade secret law."*[14]

In the opposite extreme, there are situations where one can violate trade secret law even though the information is not technically a trade secret. This occurs when one has learned the information in the context of a confidential relationship which he then violated.

Consider the following case: *A* approaches *B* expressing his interest to sell *B*'s product. *A* falsely claims a sales force of thirteen and *B* shows *A* details about his business and product. *A* later informs *B* he would not sell *B*'s product and uses the knowledge he acquired from *B* to produce and market a similar product. *B* sues *A*, who argues that the information provided by *B* was not trade secret information. The court held:

> *"It is doubtful whether [A] ever in good faith intended to sell [B's] product . . . the essence of [A's] action is not infringement but breach of faith. It matters not that [A] could have gained their knowledge from a study of the expired patents and plaintiff's publicly marketed product. Instead they gained it from [B] via their confidential relationship, and in so doing incurred a duty not to use it to [B's] detriment. This duty they have breached."*[15]

Consider the following two pre-EEA trade secret cases:

1. *On February 2, 1996, a Japanese business executive obtained confidential information from a computer chip manufacturer by posing as a Toshiba representative, knowing that the target company had a confidential relationship with Toshiba. The man was subsequently arrested by the FBI, pled guilty to a felony charge, sentenced to time served, and was deported.*[16]
2. *In September 1996, a private investigator approached a target company posing as a graduate student and claimed to need the company's confidential information for his research. The company provided the information after the "student" agreed to signing a non-disclosure agreement, which he violated by providing his client with the information.*[17]

It is hard to imagine that properly trained CI professionals would not understand that the activity in these cases clearly violates trade secret law. When CI professionals recognize or have a visceral feeling that a certain type of pretext activity is illegal, it is of the sort described in the above-two examples, a misrepresentation that induces a breach of confidence. Competitive intelligence "gray zone" hypotheticals do not entail the type of improper behavior anticipated by trade secret law.

COMPETITIVE INTELLIGENCE "GRAY ZONE" HYPOTHETICALS DO NOT ENTAIL THE TYPE OF IMPROPER BEHAVIOR ANTICIPATED BY TRADE SECRET LAW

Several specific issues need be addressed with respect to the EEA and CI.

A. *The argument has been made that the EEA's much broader definition of a trade secret presents new dangers to those seeking competitive intelligence.*

True, the EEA's definition is broader than previous legal definitions. That is because a criminal statute should be written in explicit language to give notice as to what it criminalizes, otherwise it risks being declared unconsti-

tutional. In practice, however, the decision as to what constitutes a trade secret is not based solely on the wording of a statute but on how courts have interpreted those words. I do not know anyone who would steal a trade secret on the calculation that pre-EEA case law and statutes in the jurisdiction in which he would be tried do not cover the subject-matter of the theft.

B. Perhaps the most blatant misrepresentation of law can be found in the article "How Safe Are Your Secrets" published in the September 8, 1997 edition of Fortune *magazine*

Citing several hypotheticals, one them overhearing two competitors talk loudly on an airplane, *Fortune* stated "Such shenanigans are now illegal or probably illegal, since the EEA defines theft as the knowing misappropriation of a secret without its owner's consent . . . Are we saying you're obligated, now, to protect your competitors from their own stupidity? Yes."

There is absolutely no legal basis for the proposition that one must protect a competitor from his own stupidity. If however, the EEA prohibits the taking of a trade secret without the owner's consent, does one then break the law by picking up a confidential document left by a competitor in the street?

The answer is clearly of course not. Though the ethical standard would recommend to return it, a document left on the street has lost its trade secret protection. You did not receive the owner's consent to pick it up, but then again you did not need his consent to begin with.

C. Calls for "EEA compliance plans" based on the Federal Sentencing Guidelines are misleading.

The Sentencing Guidelines do not instruct, dictate, require, prescribe, or obligate a company to have a compliance plan. The Sentencing Guidelines, the manual by which federal judges must sentence a defendant, allows the judge to deduct "points" from the sentence, i.e., lessen the sentence, if a *corporate defendant,* not an *individual defendant,* took measures to "detect and prevent" the criminal activity from occurring.[e] A proper compliance can lower the sentence of a *corporation* convicted of a crime; it has no relevance to the sentencing of an *individual* convicted of a crime.[f]

The Sentencing Guidelines do not actually use the "phrase compliance plan." This is the term which has developed to refer to the measures to "detect and prevent" violations of law. A company that does not have a compliance plan is not "in violation" of the Federal Sentencing Guidelines, and if not convicted of a particular crime, the lack of a compliance plan for that aspect of law will be of no consequence. Conversely, a company convicted of a federal crime will not be penalized for not having a compliance plan but will lose its chance of receiving a lowered sentence. Though not a legal requirement under the Guidelines, in practice having a compliance plan is the responsible and indeed the expected way for a company to conduct its affairs.

DOES THE EEA PROHIBIT PICKING UP A CONFIDENTIAL DOCUMENT LEFT BY A COMPETITOR IN THE STREET? OF COURSE NOT.

Generally speaking, compliance plans are geared to aspects of law that are industry specific and encompass regulations. Banks will have a compliance plan for Treasury Department regulations, pharmaceutical companies for FDA regulations, securities dealers for SEC regulations, and telecommunications companies for FCC regulations. There are no "EEA regulations" to *comply with.* One is to learn what not to do and not do it. As the activities the EEA criminalizes are substantially the same activities which CI professionals should never have been engaged in, an EEA "compliance plan" should not be substantially different from the existing professional guidelines a CI firm would be expected to have.

Finally, a compliance plan is not a document entitled "compliance plan" printed on company letterhead. CI practitioners will never learn how to "navigate the gray zone" by studying corporate compliance plans. The best "compliance plan" for CI professionals is to understand basic trade secret law.

D. The article "A Brief Compliance Manual," published in Competitive Intelligence Review *[Vol. 9(1)] contains one glaring error regarding misrepresentation.*

[e]The list of seven "must haves" from the Sentencing Guidelines, referred to in EEA compliance plan articles and presentations are not obligatory (i.e., "The organization must have established compliance standards and procedures . . . the organization must have taken steps to communicate effectively its standards and procedures to all employees and other agents . . ."). The document is talking to the judge, not the corporate defendant. The corporate defendant "must have" taken these steps for the judge to find that a reasonable plan to "detect and prevent" crime was in place, not that the company "must have" done these things as an independent legal obligation.

[f]See the annual reports of the United States Sentencing Commission for a perspective on corporate and individual sentencing. The statistical data contained in the reports show, for example, that there were over 40,000 criminal sentences in federal courts in 1994, of which under 400 involved corporate defendants.

The article's "Fraud" section presents an MBA student who also works, who approaches his employer's competitor for an interview and introduces himself only as a student. Citing the section 529 of the Restatement of Torts, the article concludes that "Stating the truth in so far as it is misleading because a qualifying matter has been omitted, is a fraud."[18]

The article quotes other legal sources supporting the proposition that "If one speaks, 'he must disclose enough to prevent his words from being misleading' "[19] and "It is now quite clear that a half truth is as bad as a lie."[20]

It is incorrect to apply these legal sources to the MBA student hypothetical. A half-truth can be "as bad as a lie" when one is under a legal duty to tell the truth, such as the seller's obligation to the buyer in the context of a business transaction. True, section 529 of the Restatement explains that "A statement containing a half-truth may be as misleading as a statement wholly false," but continues "Whether or not a partial disclosure of the facts is a fraudulent misrepresentation depends upon whether the person making the statement knows or believes that the undisclosed facts might affect the recipient's conduct in the *transaction* in hand" (*emphasis added*). The Restatement offers examples such as a prospectus that accurately states assets but omits "any reference to its floating debt," "a statement by a vendor that his title has been upheld by a particular court is a false misrepresentation if he fails to disclose his knowledge that an appeal from the decision is pending," and "one who offers land or a chattel for sale on inspection by so doing impliedly asserts that he knows of nothing that makes the appearance of the article deceptive."

Prosser and Keeton similarly relate the "half-truth" rule to business transactions: "Merely by entering into some *transactions* at all, the defendant may reasonably be taken to present that some things are true," and cites as examples "turning back the odometer of an automobile offered for sale" or "stacking aluminum sheets to conceal corroded ones in the middle" (*emphasis added*).

True again, that Prosser and Keeton state: ". . . if the defendant does speak, he must disclose enough to prevent his words from being misleading," but cites as examples "the rental of a property which does not mention that it is illegal," or "the income of an amusement center which does not disclose that there has been a police raid which is likely to affect it."

The text from which "It is now quite clear that a half truth is as bad as a lie"[20] qualifies it with the following illustration: "Thus, in 1932 a British court sent Lord Kylsant to prison because his steamship line had issued a prospectus that truthfully stated its average net income for the past ten years and its dividends for the past 17 years, but had deliberately concealed the fact that its earnings during the first three years of the ten years had been greatly augmented by World War I as compared with the seven lean years that followed."

To strengthen my analysis, I performed the following search: <res! /3 torts /5 529 and trade secret> of all federal and state cases on the Lexis system, which showed that there are no trade secret cases citing this section of the Restatement.

In short, the article presents the law of fraudulent misrepresentation without clarifying that it applies to situations where one has a legal duty to tell the truth, such as the seller in a business transaction.

THE LAW OF FRAUDULENT MISREPRESENTATION APPLIES TO SITUATIONS WHERE ONE HAS A LEGAL DUTY TO TELL THE TRUTH, AS THE SELLER IN A BUSINESS TRANSACTION.

E. *The purpose of Peter Kalitka's article "Are Competitor Intelligence 'Professionals' Trying To Have It Both Ways?"* (CIR *9(3):* 25-29) *is apparently to warn the CI community to beware of people who argue that the EEA is necessary to combat efforts of those stealing American trade secrets and who are at the same time teaching CI professionals how to exploit weaknesses in their competitors.*

This thesis can be dismissed by simply noting that because information collection techniques are aggressive does not necessarily make them illegal.

Mr. Kalitka also makes reference to the three-hour workshop I delivered on the topic of CI and the EEA at SCIP's 1998 Annual Conference by writing of "discussion forums designed to understand 'why the EEA of 1996 was never intended to apply to CI professionals'? Really? Doesn't the law apply equally to everyone under the jurisdiction of that law or are CI professionals to be given 'gray area' immunity?"

The exact reference in the convention brochure stated that I would "show why the EEA was never intended to apply *to the CI profession.*" As I would expect one who understands the statement in its original to mean that identification as a CI professional allows for an exemption from a federal law to not be the sort to contemplate the practical significance of the EEA. I therefore conclude that Mr. Kalitka has for whatever reason significantly mischaracterized my presentation.

Perhaps most disturbing is Mr. Kalitka's critique that some CI professionals "skirted ethics" because they knew that "ethical rules were not policed or enforceable," this particularly in light of the fact that Mr. Kalitka actually criticized SCIP's Code of Ethics as being "so broad and so general, that in several cases it encourages a variety of interpretations."[21]

What comes to my mind is the following: *A* loans *B* his weapon. Does *B*'s ethical obligation to return *A*'s weapon to him apply even if *A* "subsequently went out of his mind?"—answered in the negative in *Republic* by Plato.[22] Jump to the twentieth century, where in "*The Other America: Poverty in the United States,*" Michael Harrington relates the following story: An employer knows that employee's drinking problem is so severe that one more bout with alcohol could kill him. Concerned that employee will purchase liquor, come pay day the employer decides nonetheless to pay the employee his earned wages, who spends it on alcohol and dies the following day from intoxication.

I cite these examples to demonstrate that questions which have been analyzed since human intellect first took an interest in ethics have relevance for contemporary situations, making the notion of policing ethics after discouraging other interpretations a dangerous one indeed.

THAT INFORMATION COLLECTION TECHNIQUES ARE AGGRESSIVE DOES NOT NECESSARILY MAKE THEM ILLEGAL.

Misapprehensions

I believe it is only a matter of time for the CI community to recognize that the initial public reaction to the EEA was based on misapprehensions rather than a reasoned understanding of trade secret law. Assertions such as the one made by "a large-firm California IP litigator, who spoke on the condition of anonymity" that he "suspect(s) that the [EEA] was pushed by out-of-work FBI people now that the Cold War has slowed down"[23] or that "industry has pushed hard for [the EEA] because it perceives a decline in employee loyalty"[24] will be looked back at as amusing.

As to how ideas take on a life of their own and become rumors, myths, or fears, see *Extraordinary Popular Delusions and the Madness of Crowds* by Charles Mackay (originally published in London in 1841), *The Natural History of Stupidity* by Paul Tabori (a serious piece of scholarship despite its name), and *The True Believer* by Eric Hoffer.

Perhaps, the most important lesson to be learned from this matter is that the ethical standard is more restrictive than the legal standard. Properly trained CI professionals who recognize what this standard means and have incorporated it into their business practice need not be distracted or concerned by the EEA debate.

Finally, I encourage those who disagree with any part of my analysis to critique or challenge it in writing.

Endnotes

1. "New Spy Law Could Cramp Economy," *USA Today,* February 20, 1997.

2. "New Spy Act to Boost White-Collar Defense Biz," *The National Law Journal,* July 28, 1997, p. A1.

3. "Go Directly to Jail: New Federal Law Protects Trade Secrets," *New Jersey Law Journal,* March 9, 1998, p. 32.

4. "U.S. Economic Espionage Act: Tough EEA Enforcement Reveals Need for Strict Compliance," *Business Crimes Bulletin,* January 1998, p. 4.

5. Fine, N. (February 1998) "The Economic Espionage Act: A Wake-Up Call," *SCIP 2nd Annual Symposia on Ethics and the Law Proceedings,* p. 15.

6. Fine, N. (February 1998) "The Economic Espionage Act: Turning Fear Into Compliance," *SCIP 2nd Annual Symposia on Ethics and the Law Proceedings,* p. 135; also *Competitive Intelligence Review,* 8(3):20.

7. "Economic Espionage Act: A Whole New Ball Game," *New York Law Journal,* January 2, 1997, p. 5.

8. Pooley, J. (Fall 1997) "Criminal Consequences of Trade Secret Theft: The EEA and Compliance Plans," *SCIP EEA Symposia Proceedings;* also *Competitive Intelligence Review,* 8(3):13.

9. Fine, N. *SCIP EEA Symposia Proceedings,* February 24–35, 1997, section 3, p. 18.

10. Economic Espionage Act of 1996: Implications and Protective Measures to be Addressed at CSI NetSec '97, *PR Newswire,* February 25, 1997.

11. See footnote a.

12. See Congressional Records of October 2, 1996, S12214.

13. Section 757, comment a.

14. *Defiance Button Mach. Co.* v. *C&C Metal Products,* 759 F.2d 1053, 1063–1064 (2d Cir. 1985).

15. *Franke* v. *Wiltschek,* 209 F.2d 493, 494–495 (2d Cir. 1954).

16. "Ex-Silicon Valley Executive Held in Plot to Steal Secrets," *The San Francisco Chronicle,* March 8, 1997; "Japanese Man Arrested On Corporate Spy Charges, *Agence France Presse,* March 8, 1997; "FBI Arrests Japanese Man On High-Tech Fraud Charges," *Reuters North American Wire,* March 8, 1997; "Man Posed As Toshiba Worker To Obtain Data, FBI Says," *Electronic Buyers' News,* March 17, 1997; "Ex-Linear Japan Exec Deported In Fraud Case," *Electronic News,* June 2, 1997.

17. "Atlantan In Corporate Spy Case," *The Atlanta Journal and Constitution,* May 10, 1997; "New River Textile Maker Accuses Big Rival of Spying," *Roanoke Times & World News,* May 16, 1997; NRB Industries v. R.A. Taylor & Associates et al., Second Amended Complaint, No. 97 Civ. 0181, p. 43.

18. *Competitive Intelligence Review,* (9)1:31.

19. *Prosser and Keeton on Torts, 5th ed.,* 1984, p. 738.

20. L. Loss and J. Seligman, *Securities Regulation,* 9A.2.

21. Kalitka, P. (Fall 1997) "Counterintelligence and Law Enforcement: The Economic Espionage Act of 1996 versus Competitive Intelligence," *Competitive Intelligence Review,* 8(3):27.

22. Plato (1987) *The Republic,* p. 66, New York: Penguin Books.

23. "New Spy Act To Boost White-Collar Defense Biz," *The National Law Journal,* July 28, 1997, p. A18.

24. "Intellectual Property Concerns Overdone, Not Half-Baked" *Research-Technology Management,* March/April 1998.

About the Author

Richard Horowitz is an attorney concentrating in corporate, security, and international issues. He holds a private investigator's license and served in the Israel Defense Forces with the rank of captain. He is a member of SCIP, and can be reached at 420 Madison Avenue, Suite 300 New York, NY 10017; Tel: (212) 829-8196; Fax: (212) 829-8199; or RHESQ@Compuserve.com.