

Competitive Intelligence and the Economic Espionage Act

**A Policy Analysis Adopted by the SCIP Board of Directors
and Written by Richard Horowitz, Esq.
with Letters of Endorsement**



**Society of Competitive Intelligence Professionals
1700 Diagonal Road, Suite 600
Alexandria, VA 22314 USA
www.scip.org**

Copyright © 1999 by SCIP

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

Introduction

In October 1996, the U.S. president signed into law the Economic Espionage Act (EEA). The EEA makes stealing or obtaining trade secrets by fraud (and buying or receiving secrets so obtained) a U.S. federal crime. Upon passage of the EEA, some members of the competitive intelligence (CI) community expressed concern that the EEA could have implications for the conduct of CI.

After the passage of the EEA, SCIP organized two symposia, one in February 1997 and another in February 1998, on the topic of CI, ethics, and law. The purpose of these events, and of several publications and articles published by SCIP, was to promote education and understanding of the law and its implications for the CI profession among SCIP's membership and in industry at large.

Many members of the Society felt it was important to develop a clear statement to define the impact of the EEA on the CI profession and clear up any confusion about the relationship between the EEA and CI. This policy statement, the result of extensive research and consultation, addresses that relationship. The policy statement was prepared by Richard Horowitz, a SCIP member who is an attorney and private investigator. It was subsequently adopted by the SCIP board of directors and endorsed by leading legal experts. Their endorsements are also included in this booklet.

Competitive intelligence is the legal and ethical collection and synthesis of data and information to enhance business decision making. SCIP members endorse this definition.

— Ava Harth Youngblood, SCIP '98-99 president

SCIP Code of Ethics for CI Professionals

- To continually strive to increase respect and recognition for the profession.
- To pursue one's duties with zeal and diligence while maintaining the highest degree of professionalism and avoiding all unethical practices.
- To faithfully adhere to and abide by one's company's policies, objectives and guidelines.
- To comply with all applicable laws.
- To accurately disclose all relevant information, including one's identity and organization, prior to all interviews.
- To fully respect all requests for confidentiality of information.
- To promote and encourage full compliance with these ethical standards within one's company, with third party contractors, and within the entire profession.

Introduction to the SCIP Policy Analysis on Competitive Intelligence and the Economic Espionage Act

Richard Horowitz, Esq.
Attorney at Law
450 Seventh Avenue, 9th Floor
New York, NY 10123, USA
Tel.: +1.212.829.8196
Fax: +1.212.813.3214
rhorowitz@rhesq.com

Under the auspices of the SCIP ethics committee and as requested by the SCIP board of directors, I have prepared this policy analysis, adopted by SCIP's board of directors.

The question of the EEA's effect on CI has been an issue of concern in the CI industry. I believe that the significant difficulty for many in understanding what effect if any the EEA has on CI is that this issue reflects a confluence of law and security, two topics that are not generally included in a college or graduate school education. For example, the EEA is a statute, and a statute is not prose. Statutes are written without incorporating the underlying legal principles into their wording. The frustration many have felt after reading the EEA and still not understanding how it affects CI is because these underlying legal principles which are essential to understanding the law's application will not emerge from the text, regardless of fonts, graphics, or the statute's layout on the page.

I have always maintained that CI practitioners who act consistently with SCIP's code of ethics should not run afoul of the EEA. It is my hope that this policy analysis will assist members of the CI industry to understand why this is so. For those who would like a more in-depth analysis, see my article "The Economic Espionage Act: The Rules Have Not Changed" in the July-September 1998 volume of *Competitive Intelligence Review*.

I would like to thank Elkan Abramowitz, Mark Halligan, Peter Toren and the board of directors and staff of SCIP for their assistance in the preparation of this document. A special thanks to Mark, Peter and Hamilton Loeb for their assistance to me since I took an active role in this issue. In case there are any further questions, I can be reached at the address above.

Richard Horowitz

POLICY ANALYSIS

Competitive Intelligence and the Economic Espionage Act

Prepared by Richard Horowitz, Esq.

For the board of directors of Society of Competitive Intelligence Professionals

Executive Summary

Seeking competitive information in a legal and ethical manner is an integral component of healthy competition.

The EEA was enacted in order to enable federal law enforcement to investigate and prosecute acts of economic espionage. It adds federal criminal penalties to activities which were already illegal under state law. The EEA does not interfere with the way corporations are entitled to gain a competitive advantage in the marketplace by seeking information on a competitor in a legal manner.

That the EEA does not materially affect competitive intelligence (CI) does not mean that CI professionals need not be concerned about trade secret law. On the contrary, the EEA has drawn attention to the necessity of insuring that CI activities are within the parameters of trade secret law.

An understanding of trade secret law and the EEA indicates that CI professionals who have been and will continue to conduct their business in an ethical manner and consistent with established trade secret law need not be concerned about the EEA debate.

Companies that have curtailed their CI efforts out of a misplaced fear of the EEA have awarded a competitive advantage to companies whose CI activities continue unimpeded.

Background

The Society of Competitive Intelligence Professionals (SCIP) is the global professional society for practitioners of business or competitive intelligence (CI). Established in 1986, SCIP today has more than 5,000 members and continues to grow substantially year after year.

Seeking information on a competitor is an important component of healthy competition; CI is the term which has developed to describe this profession. Many corporations and executives perform this function without any formal ties to the CI profession, while others employ CI professionals or outside CI firms and practitioners. Many large corporations have established entire CI departments. Competitive intelligence is a recognized,

accepted, and legal way for businesses to gain a competitive advantage in the marketplace. This in turn accelerates the benefits to society of competition in the marketplace.

SCIP encourages its members to abide by its code of ethics; one clause in the code instructs its members to "accurately disclose all relevant information, including one's identity and organization, prior to all interviews."

The Economic Espionage Act of October 1996 (EEA) was enacted by the U.S. Congress in response to attempts by foreign entities to steal American trade secrets. It was not enacted in order to regulate the CI industry nor was it enacted in response to any problems arising out of the activities of CI professionals. Its passage however has led to various and sometimes conflicting opinions regarding the EEA and has created confusion regarding its implications for the practice of CI.

The EEA is a federal criminal law and was passed in order to enable federal authorities to investigate and prosecute acts of economic espionage.

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

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 had always been prohibited under state law and/or inconsistent with 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.

Implications

There are several reasons why the EEA should not have any impact on the practice of competitive intelligence.

First, the act of seeking and collecting information on a competitor is itself legal. Note the following from the Restatement of Torts (1939):

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 (Section 757, Comment a).

One limitation on this rule cited by the Restatement is: "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."

Information collection performed by CI professionals centers around the sophisticated use of published material, databases, and on-the-record interviews, techniques which themselves are legal and proper means of acquiring information.

Second, properly trained CI professionals who have conducted themselves in an ethical manner were not engaged in legally risky business prior to the EEA. The appropriate legal principles have been instilled into the CI profession over the years of its existence and subsequently adopted as practice by properly trained industry members. The increased penalties for trade secret theft under the EEA will not be applicable to those whose practice has been consistent with the already existing legal standards.

Third, most situations commonly referred to as "gray zone" areas are not trade secret violations at all. Though they raise ethical questions, "gray zone" situations such as 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 which alone will not trigger trade secret liability. Properly trained CI professionals should be able to identify and avoid the predicaments that would place them in actual legal risk.

Fourth, the EEA will not be applied to general commercial disputes, but to clear criminal acts of theft. The reason for the EEA's passage was to thwart attempts at stealing American trade secrets which would have an impact on the competitiveness and health of the American economy. That the U.S. Attorney General promised Congress that no charges will be filed under the EEA for the first five years after the law's enactment without the approval of the Attorney General or two of her top deputies indicates that federal authorities have no intention of becoming entangled in the numerous trade secret disputes that do take place in the routine course of business (see Congressional Record, October 2, 1994, S12214).

To summarize, the EEA incorporates into the federal criminal code activities that were already illegal under state law. It does not add new burdens or restrictions to the American workforce.

A Note on Extraterritoriality

About twenty percent of SCIP's membership is outside the USA, making the question of how the EEA affects overseas activity pertinent.

The EEA does have an extraterritoriality clause. In principle, a statute must state that it applies overseas for it to so apply. The extraterritoriality provisions of the EEA apply the statute to a U.S. citizen even abroad, and to a non-U.S. citizen (1) while on U.S. soil or (2) abroad, if the act committed abroad violates the EEA and "an act in furtherance of the offense was committed in the United States."

What this means in practice is that whatever types of activities the EEA prohibits overseas are the same as what is prohibited on U.S. soil, which, as explained, had always been prohibited by state law and/or inconsistent with SCIP's code of ethics.

EEA Compliance Plans

An additional reason for concern regarding the implications of the EEA on competitive intelligence has been the many calls for "EEA compliance plans" based on the Federal Sentencing Guidelines. 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. 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.

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 in order 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.

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.

There are no "EEA regulations" to *comply with*. One is to learn what not to do and not do it. 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. As the activities the EEA criminalizes are substantially the same activities in which CI professionals should never have been engaged, an EEA "compliance plan" should not be substantially different from the existing professional guidelines a CI firm or professional would be expected to have or abide by.

Answers to Frequently Asked Questions

1. Even if the EEA was not intended to deal with competitive intelligence or general commercial disputes, hasn't it had an impact nonetheless?

Answer: The impact the EEA has had on the CI community has been based on anxiety and confusion. Some companies have mistakenly taken the position that the EEA has placed them in legal jeopardy because of the activities of their CI professionals.

Ironically, companies who curtail the legal and ethical activities of their CI professionals have placed themselves at a competitive disadvantage to companies whose CI activities continue unimpeded.

2. Don't we have to wait to see how the EEA is applied in the courts before determining what it prohibits?

Answer: How courts ultimately interpret statutes is a fundamental part of legal analysis. This does not mean however that one cannot understand the basic prohibitions of a statute. In fact, a statute can be declared unconstitutional by the courts if it does not provide adequate notice as to what it prohibits.

The intention and purpose behind the EEA was clearly explained by Congress prior to its enactment. This did not include an intention to alter the fundamentals of corporate conduct, but to deter and punish the criminal act of trade secret theft.

3. Can't the EEA be applied to situations it was not intended to cover?

Answer: It is not unusual for some laws to ultimately be applied to unforeseen situations. A law once passed may take on a life of its own. The concern that the EEA will be applied to routine commercial disputes was discussed and dismissed by Congress prior to the EEA's passage, with the Attorney General's letter giving further assurances to this effect (see page 4). Companies who remain concerned are well-advised to study the background of the law.

4. The definition of a trade secret under the EEA is broader than existing trade secret law. What implications does this have on competitive intelligence?

Answer: The wording of the EEA's definition enumerates more types of information considered a trade secret than previous legal definitions. This is because a criminal statute should be written in explicit language so as to give notice as to what it criminalizes, otherwise it risks being declared unconstitutional. This does not mean that prior legal definitions excluded types of information enumerated in the EEA's definition.

In practice, existing legal definitions and case law interpretations cover all sorts of financial, business, and scientific information.

Whether the information stolen is included in the EEA's definition of a trade secret is moot with respect to professionals whose conduct precludes them from engaging in theft.

5. What effect if any does the EEA have on the legal risks one may decide to take in seeking information on a competitor?

Answer: The EEA compounds the legal consequences for one engaged in theft of a trade secret by adding federal criminal penalties to an act which already triggers state civil penalties. This added risk however is of no consequence to one who seeks information on a competitor in a legal manner.

6. What implication does the EEA have on a company's efforts to protect information?

Answer: The EEA focuses primarily on the activities it prohibits. The EEA's definition of a trade secret however, like state trade secret law preceding it, requires the trade secret holder to take reasonable measures to keep that information secret. In practice, the holder of a trade secret must have taken those reasonable measures in order for one who misappropriates that information to be held liable under the EEA or state trade secret law.

WELSH & KATZ, LTD.

Attorneys at Law

A. SIDNEY KATZ*
RICHARD L. WOOD*
JEROLD B. SCHNAYER
ERIC C. COHEN
JOSEPH R. MARCUS
GERALD S. SCHUR
GERALD T. SHEKLETON
JAMES A. SCHEER
DANIEL R. CHERRY
ROBERT B. BREISBLATT
JAMES P. WHITE
R. MARK HALLIGAN
HARTWELL P. MORSE, III
EDWARD P. GAMSON, PH.D.
KARA E.F. CENAR
KATHLEEN A. RHEINTGEN
THOMAS W. TOLPIN*
ELLIOTT C. BANKENDORF
RICHARD W. McLAREN, JR.
JOHN L. AMBROGI
JULIE A. KATZ
JON P. CHRISTENSEN

120 SOUTH RIVERSIDE PLAZA • 22ND FLOOR
CHICAGO, ILLINOIS 60606

TELEPHONE (312) 655-1500
FACSIMILE (312) 655-1501

ERIC D. COHEN
WALTER J. KAWULA, JR.
LEONARD FRIEDMAN
STEVEN E. FELDMAN
IK HYUN SEO
PHILIP D. SEGREST, JR.
JEFFREY W. SALMON
MITCHELL J. WEINSTEIN
SHANNON L. NEBOLSKY, PH.D.
ELIZABETH D. McGOOGAN
RICHARD J. GURAK
SCOTT M. GETTLESON
J. ARON CARNAHAN
MICHAEL A. BONDI
RALPH E. KRISHER III
THOMAS L. GEMMELL
LOUISE T. WALSH

OF COUNSEL
DONALD L. WELSH
LAURIE A. HAYNIE

WASHINGTON OFFICE
CRYSTAL PLAZA ONE • SUITE 206
2001 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VIRGINIA 22202-3603
TELEPHONE (703) 415-4777

January 21, 1999

* ALSO ADMITTED IN DISTRICT OF COLUMBIA

VIA OVERNIGHT COURIER

SCIP Board of Directors
Society of Competitive Intelligence Professionals
1700 Diagonal Road
Suite 520
Alexandria, Virginia 22314

Re: Competitive Intelligence and the Economic Espionage Act

Dear Board Members:

As you know, I teach trade secrets law at John Marshall Law School and I am an active practitioner and retained expert in trade secret cases around the country. See <http://www.execpc.com/~mhallign/resume1.html>.

At Richard Horowitz's request, I have reviewed his (8/17/98) draft entitled "Proposed Policy Analysis: Competitive Intelligence and the Economic Espionage Act."

This is a well written draft and I endorse it. I strongly agree with the basic underlying premise -- The EEA does not materially affect competitive intelligence activities and companies should not curtail competitive intelligence activities based on a "misplaced fear" of the EEA. In fact, just the opposite is true. Companies should increase competitive intelligence activities to meet the challenge of an increasingly global competitive environment.

My summary of "Reported Criminal Arrests Under the Economic Espionage Act of 1996" is the most up-to-date information available on EEA prosecutions and convictions. It is available on the Internet at <http://www.execpc.com/~mhallign/indict.html>. As you can see, these EEA prosecutions involve trade secret theft and bear no reasonable relationship whatsoever

SCIP Board of Directors

February 11, 1999
Page 2

to legitimate competitive intelligence activities.

If I can be of further assistance to the SCIP Board of Directors, please contact me at 1-312-526-1559.

Very truly yours,

R. M-L H —

R. Mark Halligan

RMH/js

cc: Richard Horowitz, Esq.

Peter J. Toren
525 University Ave.
Palo Alto, CA 94301

SCIP Board of Directors
Society of Competitive Intelligence Professionals
1700 Diagonal Road
Suite 520
Alexandria, VA 22314

Re: Economic Espionage Act of 1996

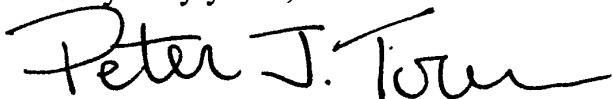
Dear Board Members:

I was formerly a trial attorney with the Computer Crime and Intellectual Property Section of the United States Department of Justice where I was involved in drafting the Economic Espionage Act of 1996 ("EEA"), and was the lead prosecutor on one of the first cases brought under the EEA. In addition, I am a co-author of an article entitled "Understanding the Economic Espionage Act of 1996," 5 Tex. Int. Prop. L.J. 177 (Winter 1997). Currently, I am a Special Counsel in the San Francisco and Palo Alto offices of Heller Ehrman White and McAuliffe.

At Richard Horowitz's request, I have reviewed SCIP's "Proposed Policy Analysis: Competitive Intelligence and the Economic Espionage Act" and offer the following comments.

The EEA was intended to address both the general need for a federal criminal deterrent against trade secret theft and the apparent threat of industrial espionage sponsored by foreign countries. The EEA was not intended to impose new restrictions on American businesses. I agree with the Policy Analysis that the EEA was not developed in order to regulate the competitive intelligence community, nor was it developed in response to any problems that might have existed in the competitive intelligence community. Competitive intelligence practitioners who abide by SCIP's Code of Ethics should not be in violation of the EEA. If I can be of further assistance to the SCIP Board of Directors, please call me at (650) 324-7156 or e-mail me at bmtsdad@AOL.com.

Very truly yours,



Peter J. Toren

MORVILLO, ABRAMOWITZ, GRAND, IASON & SILBERBERG, P.C.

ELKAN ABRAMOWITZ
ROBERT J. ANELLO
LAWRENCE S. BADER
BARRY A. BOHRER
CATHERINE M. FOTI
PAUL R. GRAND
LAWRENCE IASON
ROBERT G. MORVILLO
DIANA D. PARKER
MICHAEL C. SILBERBERG
EDWARD M. SPIRO
JOHN J. TIGUE, JR.
RICHARD D. WEINBERG

COUNSEL
ROBERT J. MC GUIRE
MICHAEL W. MITCHELL

565 FIFTH AVENUE
NEW YORK, N.Y. 10017
TELEPHONE
(212) 856-9600
CABLE: LITIGATOR, NEW YORK
FACSIMILE
(212) 856-9494
WRITER'S DIRECT DIAL
880-9500

March 2, 1999

DAVID AXINN
ANIRUDH BANSAL
NEIL M. BAROFSKY
DAVID A. BATTAT
STEVEN H. BRESLOW
MICHAEL F. BUCHANAN
JAMES C. DUGAN
REBECCA A. GLASER
R. JOSEPH GRIBKO
RACHEL M. HEALD
MICHAEL R. MARRA
MARC E. MASTERS
HELEN L. MONACO
GRETCHAN R. OHLIG
JODI MISHER PEIKIN
MAE C. QUINN*
JOSHUA H. REISMAN
ELIZABETH SMALL
PETER M. SPETT
JOSEPH C. SPONHOLZ
ALISON VAN HORN

*ADMITTED ONLY IN DISTRICT OF COLUMBIA

BY FEDERAL EXPRESS

SCIP Board of Directors
Society of Competitive Intelligence Professionals
1700 Diagonal Road
Suite 520
Alexandria, VA 22314

Re: Economic Espionage Act of 1996

Dear Board Members:

I am a former Chief of the Criminal Division of the United States Attorney's Office for the Southern District of New York and co-author of the chapter entitled "Corporate Sentencing Under the Federal Guidelines," in Obermaier and Morvillo, White Collar Crime: Business and Regulatory Offenses.

At Richard Horowitz's request, I have reviewed his (1/27/99) draft entitled "Proposed Policy Analysis: Competitive Intelligence and The Economic Espionage Act," particularly the section dealing with the sentencing guidelines and compliance plans.

Mr. Horowitz has written an interesting and informative submission, pointing out the relationship between compliance plans and the Federal Sentencing Guidelines as they relate to corporations. His analysis is incisive and important.

SCIP Board of Directors

- 2 -

March 2, 1999

I agree with his analysis that the Federal Sentencing Guidelines do not create a legal obligation for a corporation to create a compliance plan.

If I can be of further assistance to the SCIP Board of Directors, please feel free to contact me at the above number.

Very truly yours,

Elkan Abramowitz /MB

EA/cs

Elkan Abramowitz

cc: Richard Horowitz, Esq.

