

# Competitive Intelligence, Law, and Ethics: The Economic Espionage Act Revisited Again (and Hopefully for the Last Time)

*Richard Horowitz, Esq.*

Several years ago, when SCIP asked me to publish another article on law and ethics, I responded that I believed I had already written everything I thought competitive intelligence professionals needed to know. After all, the title of my 2003 *Competitive Intelligence Magazine* article was “CI, law, and ethics: The EEA revisited” (Horowitz 2003). If I had revisited the issue then (after previously publishing several pieces and giving numerous presentations at SCIP conferences and chapter meetings), what more did I need to say on the topic?

I have always unhesitatingly maintained that competitive intelligence *is not an inherently legally risky profession*. Not all lawyers agree, or will say that they do. In fact, the extent to which some lawyers portray competitive intelligence as legally risky can be viewed as misguided.

If you're a SCIP member of recent years, you may be unaware of the political debate that took place following the passage of the Economic Espionage Act (EEA) in October 1996. In hindsight, SCIP's response to the EEA should have been to simply issue a one-page statement to its members saying this new law has nothing to do with them, here's why, and let's all go back to work. Instead, SCIP held a two-day symposium in 1997 on the implications of the EEA, giving a platform to numerous

speakers who warned of the dire consequences that the competitive intelligence industry, they claimed, now faced.

With a re-emergence of the type of scare-mongering articles and presentations that were common in the years following the EEA's passage, I decided that the issue needs to be revisited, again, even though I had written for SCIP a policy analysis on competitive intelligence and the EEA in 1999. With that the matter should have been closed.

## A SHORT HISTORY

As I stated at SCIP's 1997 symposium, the EEA would have no impact on competitive intelligence firms and professionals who had been practicing in a legal and ethical manner. In 1998 I wrote “The Economic Espionage Act: The rules have not changed” and recalled what I said at the symposium:

*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 the 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. (Horowitz 1998)*

Why was I so sure?

*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. (Horowitz 1998)*

It really is this simple: the EEA gave jurisdiction to federal authorities to investigate, indict, and prosecute trade secret theft. It did not change what was or was not legal. I also included the following in my 1998 article:

*Adding to the confusion regarding the EEA has been series of articles and presentations that has created the impression that the EEA fundamentally alters how competitive intelligence professionals must conduct their affairs: "New Spy Law Could Cramp Economy (Schweizer 1997); "New Spy Act To Boost White-Collar Defense Biz (Slind-Flor 1997); "Go Directly To Jail: New Federal Law Protects Trade Secrets (Calmann 1998); "U.S. Economic Espionage Act: Tough EEA Enforcement Reveals Need for Strict Compliance (Perkins 1998); "The Economic Espionage Act: Turning Fear Into Compliance (Fine 1997); and "Economic Espionage Act: A Whole New Ball Game (Chaim 1997)."*

*Among the more notable assertions: "Your industry is crawling with criminals. And you maybe 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."*  
(Pooley 1997)

Rereading this material reminds me of what one SCIP veteran said to me ten years ago: "Apparently for lawyers, a new statute is like a new product line, you've got to market it."

- A lawyer published that "the statute [EEA] creates a new list of activities" that those providing "competitor intelligence service . . . must avoid as they pursue their day-to-day activities" (Chaim 1997). (There is no "new list of activities.")
- The opening sentence of the *National Law Journal* article entitled "New Spy Act To Boost Criminal Defense Biz" was "The new Economic Espionage Act may prove to be a field of dreams for white-collar criminal defense lawyers and firms with high-tech clients" (Abramson 1997).
- At a 1998 SCIP conference on law and ethics in Atlanta, a local lawyer actually said "none of this would be happening of this industry acted more ethically."
- In 1999, one bar association held a program entitled "Electronic Espionage Act Update" and a competitive intelligence conference (not sponsored by SCIP) contained a session which was to discuss "Litigation of Competitive Intelligence Cases," even though there hadn't been any.

The key to understanding why competitive intelligence is not inherently a legally risky profession is this: trade secret law protects the information holder from someone who 'misappropriates' a trade secret, and 'to misappropriate' means to acquire through 'improper means.' What constitutes improper means is beyond the scope of this article but suffice it to say that *you can acquire another's trade secret provided all the means you used to acquire that information were themselves legal*. It cannot be otherwise, because were that to be the case – a declaration that your information is a trade secret would prohibit others from trying to acquire it – then in effect you have given yourself perpetual intellectual property protection, thereby pre-empting federal patent law. Why patent something if a patent expires and declaring you have a trade secret prohibits others from trying to acquire it, even through legal means, without a time limitation?

I also wrote in 1998 that competitive intelligence is actually *encouraged by the law*, citing, 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)

After debates with lawyers at various conferences, SCIP asked me to write a policy analysis on the EEA which SCIP's board adopted as its policy and made public at its 1999 annual convention. The Policy Analysis contains letters of endorsement from three legal authorities, Elkan Abramowitz, Mark Halligan, and Peter Toren.

Before publishing the Policy Analysis I met with the FBI's deputy general counsel who told me that the intention of the EEA was to foster competition, not stifle competition; that the FBI is not in the business of resolving trade secret disputes; and that by enacting the EEA, there was no intention to change the intricacies of trade secret law. (I posted my exchange of correspondence, with the deputy general counsel's permission, on my website.)

And although the *National Law Journal* published that the EEA "may prove to be a field of dreams for white-collar criminal defense lawyers and firms with high-tech clients" (Abramson 1997), in 2000 it reviewed SCIP's Policy Analysis and wrote that while SCIP was "hypersensitive about suggestions that their work is espionage or industrial spying," they asked me to "prepare[d] an analysis of the new law [which] conclude[d] that its impact on legitimate competitive intelligence gathering would be negligible. Nearly four years later, it appears that Mr. Horowitz' predictions were on target" (Slind-Flor 2000).

With this background, the arguments which I have routinely made in publications and presentations should be clear:

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

- Companies who boast that they have overhauled their competitive intelligence collection methods because of the EEA are in effect saying that their collection methods prior to the EEA were questionable if not illegal.
- Rather than presenting risks and threats to corporate America, the EEA has enhanced the practice of competitive intelligence. By highlighting illegal activity, the EEA has emphasized the legality of accepted competitive intelligence techniques.

After giving presentations on competitive intelligence, law, and ethics throughout the years, I decided to give a slightly different presentation at SCIP's 2009 convention which I titled "*Is The CI Industry Obsessed With Ethics?*" The presentation's description began with:

*Ethics remains a matter of serious concern for all CI professionals and often creates distress and acrimonious debate within the CI industry. But should this be? Is the CI industry overly concerned with ethics or is what CI professionals do itself ethical?*

I gave this presentation to show that of all the information gathering professions, competitive intelligence is the most conservative in its information collection techniques yet at the same time the most preoccupied and scrutinized about law and ethics.

## RECENT DEVELOPMENTS

As stated in the opening, there is a re-emergence of articles and presentations similar to those that circulated in the years immediately after the passage of the EEA. This, arguably because many years have passed since the original EEA debate and similarly many SCIP members are unfamiliar with the issue. These arguments should be rebutted and the trend stopped. From some recent articles:

- "Keeping it Legal: Sniffing Out The Competition Can Be Tricky" (Costanza 2010). No it is not.
- "Theoretically the difference between espionage and legal information gathering is clear. In practice, it is quite difficult to sometimes tell the difference between legal and illegal methods" (Morrow 2010).

Again wrong; an incorrect characterization of the matter.

- An article entitled “When Does Research End and Industrial Espionage Begin?” claimed “There’s a fine line between spying on the competition and researching the competition” (Miller 2010). No there is not.
- Still another article – which claimed that since competitive intelligence is “a relatively new discipline, there are few standards for competitive intelligence professionals to follow” – recommended that “Competitive intelligence professionals should never purposefully seek to obtain the trade secrets or non-public/competitively sensitive information of other companies” (Millien 2010). Outright bad advice. Seek whatever information you want so long as you do nothing illegal in acquiring that information. (This issue is one where you can expect your company’s policy to delineate actionable parameters.)

Along these lines was the presentation given at SCIP’s 2010 Conference entitled “Keeping on the right side of the line: Best practices for acquiring competitive intelligence from a legal perspective,” preceded by an article on the same topic (Milligan Wexler 2009). Prior to the presentation I told SCIP that every topic these lawyers would cover will be wrong. Why did I think so? Because of the presentation’s description:

*More than ever, CI professionals need to be mindful that only intelligence that is gathered lawfully benefits their company in the long run. There may be a temptation to push the envelope or take unnecessary risks to distinguish oneself or one’s company in these economic times.*

*Why now more than ever?* Irrespective of the economy, there has never been a problem of competitive intelligence professionals being tempted to “push the envelope.” Just the opposite; too often they are afraid to do things that are in fact legal. But most relevant in the description was this: “recent cases involving theft of a trade secret or privacy violations serve as a stark reminder that CI professionals should do it right or not do it at all,” and spoke of “latest developments in privacy and trade secret law/unfair competition law as it relates to CI.”

Recall my comment on the 1999 conference session entitled “Litigation of competitive intelligence cases” which was that there hadn’t been any. Even today, there still haven’t been any ‘recent cases’ or ‘latest developments’ in law that are relevant to competitive intelligence. Nothing has changed. Competitive intelligence professionals need to know the basics of trade secret law (particularly the issue of improper means) to understand how the line between legal and illegal is drawn.

After listening to this presentation I found it contained four general flaws. First, the session covered numerous aspect of trade secret law: the definition of a trade secret, what are reasonable security precautions, liability for trade secret misappropriation under state and federal law (the EEA), liability for misappropriation for acquisition through inadvertent disclosure, and the potential for treble or exemplary damages. All except the one that is essential for competitive intelligence professionals to understand: the phrase ‘improper means.’ Understanding what constitutes improper means allows the intelligence professional to know what can be done. Without this understanding, one is unable to know how to draw the legal line and therefore will always hesitate when in fact the competitive intelligence professional should be encouraged to be aggressive, consistent with their company’s policies.

In general, the rule is that information loses its trade secret protection if the information holder, even by mistake, does not take reasonable precautions to keep that information secret. For CI professionals, cases where this principle is disputed are usually moot because the lawyers of the company that acquires actual trade secret information through the inadvertent disclosure on the part of the information holder will almost certainly return the information, if only to avoid potentially litigating the matter and the subsequent media attention.

Second, recognizing that the presenters did not mention improper means, I asked whether they agreed that one is entitled to acquire another’s trade secrets provided the means used were themselves legal, to which one presenter answered no, a clearly erroneous position. One is indeed entitled to acquire another’s trade secret provided the means used were themselves legal. Trade secret law only protects the information holder from someone who uses improper means to acquire the information: the real issue is what constitutes improper means. Saying only that one could be liable for trade secret misappropriation by acquiring a trade secret has no pedagogic value.



Note that corporate policies are almost always stricter than what the law allows one to do. In other words, the ethical standard is usually higher than the legal standard, and it is your company's policy that you have to comply with. You can expect your company's policy to prohibit certain actions that are legal. Moreover (and also beyond the scope of this paper) there is a subtle distinction in trade secret law between legal means and proper means. In my opinion what distinguishes the two is far less important than understanding what are legal means. Whatever may conceivably be considered legal but not proper means rarely occurs. In any case, it would most certainly be prohibited by your company's ethical policy.

Third, my assertion prior to this session – that if the presenters do talk of recent cases or latest developments, none of them will be relevant to CI – proved to be correct. Intelligence professionals do not need to be told that if an employee changes his employment he cannot take the trade secrets of his former employer with him, or that one cannot misrepresent his identity and sign a non-disclosure agreement to gain entry to a competitor's manufacturing plant, then surreptitiously take pictures with a cell phone knowing there are signs saying 'no pictures allowed.' There are no recent cases or latest developments of relevance to competitive intelligence.

Fourth, some of the presentation's best practices are of little value. "Always act in an ethical manner" is not helpful. "Avoid spying" – also not helpful. "Obtain information freely and honestly" – I do not know what obtaining information freely means, if anything. "Do it right or don't do it all" is meaningless advice if you do not explain what improper means are. "Rely on public information" is outright bad advice. And, after not explaining how to understand what is and is not illegal, "Arm yourself with the law, consult legal counsel."

## CLOSING OBSERVATIONS

I have already published everything I believe competitive intelligence professionals *need to know*. Now I will to share what I think are useful observations. The main issue I wish to analyze (politics and marketing aside) is what is it about trade secret law and competitive intelligence which continue to create confusion and erroneous proclamations?

First, a comment on trade secret law within the legal profession. Of the four main divisions of intellectual property law – patents, copyrights, trademarks, and trade

secrets – trade secret law receives far less attention and scholarship than the others. The first Restatement of Torts (published in 1939) has and will continue to be a primary source for relevant trade secret principles. Yet from 1900 through 1939, while hundreds of law review articles were published on patent, copyright, and trademark law, only eleven articles were published on trade secret law.

The valuable book *Understanding Intellectual Property* (Chisum 1992) devotes 397 pages to trademarks, 314 pages to patents, 311 pages to copyright, and only 56 pages to trade secrets, even while devoting 90 pages to "Other Intellectual Property Rights." A letter I received in 2002 from the worthwhile organization the American Intellectual Property Law Association reads "More than 13,000 attorneys – from patent, trademark, and copyright specialists to owners of intellectual property – have joined AIPLA." In 2010, the annual conferences of the American Bar Association's Intellectual Property Section held numerous sessions on patents, copyrights, and trademarks but only one on trade secrets while the annual convention of the Intellectual Property Owners Association held no sessions on trade secrets.

The reason for this I believe is straightforward: trade secret law is significantly less complex than the other three divisions of intellectual property. Hence it never attracted the in-depth attention and scholarship that would have given lawyers the ability to better understand how it applies to competitive intelligence.

Second, it is basic that a word or phrase in English can have a different meaning as a legal term of art. Even in case law, the phrase 'improper means' – the most important legal concept for intelligence professionals to know – does not have one definition encompassing all activities. To decide what constitutes improper means, a court at times may apply other legal principles to the facts of the case.

This brings us to an inherent characteristic of language (see Church 1961). For most people, the definition of space as that which is in between things, or that which is left when you take everything else away, would suffice. Not for Albert Einstein though; in his introduction to Max Jammer's *Concepts of Space* (1953), Einstein commented that "if two different authors use the words 'red,' 'hard,' or 'disappointed,' no one doubts they mean approximately the same thing." Not so with respect to words such as 'place' or 'space' wrote Einstein, "where there exists far-reaching uncertainty of interpretation." Similarly according to Aristotle; from the second paragraph to Book IV of his *Physics*: "The question, what is place? presents

many difficulties. An examination of all the relevant facts seems to lead to divergent conclusions.” If ostensibly simple words like ‘space’ or ‘place’ are unclear to Einstein and Aristotle, why the surprise that more complicated legal phrases need explanation to be understood.

Third, Aristotelian physics helped me understand another aspect of trade secret law and competitive intelligence. In Book Six, Chapter Four of *Physics*, Aristotle records and discusses Zeno’s Four Paradoxes (summarized in Maziarz 1968 p59). One paradox, known as the Flying Arrow, can be presented as follows: an object is at rest when it occupies the same space for the time it is there; therefore a flying arrow is at rest because at any given time it is found in the space in which it occupies. Counters Aristotle: “This is false, for time is not composed of indivisible moments.”

As Aristotle was in effect touching upon the infinitesimal, clearly the beginnings of calculus are found in Aristotelian physics, which mathematicians for generations could not develop until Isaac Newton then Gottfried Leibniz independently invented it in the late 17th century. Though he made his contribution to the development of calculus several decades before Newton and Leibniz, even Descartes wrote “ratios between straight and curved lines are not known, and I believe cannot be discovered by the human mind” (Descartes 1954). We see therefore that the human mind found it difficult to comprehend a dynamic where the value of each component is a function of the value of the other components. Under these circumstances, where is the starting point?

It then occurred to me that this mental dynamic is at play in trade secret law. Justice Oliver Wendell Holmes wrote in a 1930 U.S. Supreme Court tax law case: “the very meaning of a line in the law is that you intentionally may go as close to it as you can if you do not pass it” (Superior Oil 1930). But in trade secret law, how do you draw the line, where at times the three main issues of trade secret law – does the information qualify as a trade secret; were reasonable precautions used to keep that information secret; and were improper means used to acquire the information – may be dependent on the significance of, or may be a *function* of, the other? The mental dynamics required to make this determination are similar to calculus (though the differences between trade secret law and calculus far outweigh the similarities).

I again refer the reader to my 1998 article, “The EEA – The Rules Have Not Changed” for a basic explication of these issues.

In “The Concept of History,” Isaiah Berlin analyzes whether history should be regarded as a natural science and if so to what extent would history be considered an inductive or deductive science (Berlin, Hardy 1997). Upon reading this I thought of the intelligence cycle and came to a realization, that *intelligence is history before it happens*. As such, whether in national security or business, the analysis required of raw intelligence takes on an importance greater than the intelligence cycle itself. How unfortunate therefore is it that competitive intelligence professionals continue to be distracted, misinformed, or outright misled by those purporting to give sound legal advice, especially since the relevant trade secret law issues are far easier to explain and understand than one might think.

Competitive intelligence professionals would find it worthwhile to review this paper with their attorneys. For those of you who disagree with my analysis, I encourage you to send in your own critique.

## REFERENCES

- Abramson, Ronald (1997). “Economic Espionage Act of 1996: Theft of trade secrets addressed,” *National Law Journal*, July 28.
- Berlin, Isaiah; Hardy, Henry; Hausheer, Roger (1997). *The Proper Study of Mankind: an anthology of essays*, New York: Farrar, Straus and Giroux.
- Calmann, Arnold; Goldstein, Bruce (1998). “Go directly to jail: new Federal law protects trade secrets,” *New Jersey Law Journal*, March 9, p32.
- Chaim, A. Levin (1997). “Economic Espionage Act: A whole new ball game,” *New York Law Journal*, January 2, p5.
- Chisum, Donald S.; Jacobs, Michael A. (1992). *Understanding Intellectual Property*, (Legal Text Series) Matthew Bender.
- Church, Joseph (1963). *Language and the Discovery of Reality*, 2<sup>nd</sup> edition. Alfred A. Knopf and Random House.
- [www.amazon.com/Language-Discovery-Developmental-Psychology-Cognition/dp/B0012C89NU/ref=sr\\_1\\_4](http://www.amazon.com/Language-Discovery-Developmental-Psychology-Cognition/dp/B0012C89NU/ref=sr_1_4)

- Costanza, Mike (2010). "Keeping it legal: sniffing out the competition can be tricky," *Rochester Business Journal*, April 30.  
[www.rbj.net/article.asp?size=2&aID=183879](http://www.rbj.net/article.asp?size=2&aID=183879).
- Descartes, Rene; Smith, David; Latham, Marcia (1954). *The Geometry of Rene Descartes*, New York, Dover  
<http://www.amazon.com/Geometry-Rene-Descartes/dp/0486600688/>
- Fine, Naomi (1997). "The Economic Espionage Act: Turning fear into compliance," *Competitive Intelligence Review*, v8n3 Fall p20-24.
- Honovich, Jack (1993). "Time is ripe to overhaul traditional marketing research department," *Marketing News*, June 7.  
[business.highbeam.com/137540/article-1G1-14413177/time-ripe-overhaul-traditional-marketing-research-department](http://business.highbeam.com/137540/article-1G1-14413177/time-ripe-overhaul-traditional-marketing-research-department)
- Horowitz, Richard (1998). "The Economic Espionage Act: The rules have not changed," *Competitive Intelligence Review*, v9n3 July-August, p30- 38.  
[www.rhesq.com/CI/CIR.pdf](http://www.rhesq.com/CI/CIR.pdf)
- Horowitz, Richard (1999 ). "SCIP policy analysis: CI and the Economic Espionage Act (EEA)," *Competitive Intelligence Review*, v10n3, p84-89.  
[www.rhesq.com/CI/SCIP%20EEA%20Policy%20Analysis.pdf](http://www.rhesq.com/CI/SCIP%20EEA%20Policy%20Analysis.pdf)
- Horowitz, Richard (2003). "CI, law, and ethics: the EEA revisited," *Competitive Intelligence Magazine*, November/December v6n6 p56-57.  
[scip.org/Publications/CIMArticleDetail.cfm?ItemNumber=843](http://scip.org/Publications/CIMArticleDetail.cfm?ItemNumber=843)
- Jammer, Max (1993). *Concepts of Space: The History of Theories of Space in Physics*, New York: Dover.
- Maziarz, Edward; Greenwood, Thomas (1968). *Greek Mathematical Philosophy*, Frederick Ungar Publishing.
- Miller, Amy (2010). "Where does research end and industrial espionage begin?" *Law Technology News* June 14.  
[www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202462657486&When Does Research End and Industrial Espionage Begin](http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202462657486&When Does Research End and Industrial Espionage Begin).
- Millien, Raymond (2010). "Gathering Information on Your Competitors: Competitive Intelligence or Trade Secret Theft? (Part 2 of 2)," March 3.  
[dcipattorney.com/2010/03/gathering-information-on-your-competitors-competitive-intelligence-or-trade-secret-theft-part-2-of-2/](http://dcipattorney.com/2010/03/gathering-information-on-your-competitors-competitive-intelligence-or-trade-secret-theft-part-2-of-2/).
- Morrow, Frank (n.d.). "Interview with Phil Agee," (video). (Posted June 26, 2010)  
[www.publiccourtrecordssearch.com/cia-economic-intelligence-and-industrial-espionage](http://www.publiccourtrecordssearch.com/cia-economic-intelligence-and-industrial-espionage)
- Perkins, L. (1998). "US Economic Espionage Act: Tough EEA enforcement reveals need for strict compliance," *Business Crimes Bulletin: Compliance and Litigation*, January p4.
- Pooley, James (1997). "Criminal consequences of trade secret theft: The EEA and compliance plans," *Competitive Intelligence Review*, v8n3 Fall, p13-19.
- Schweizer, Peter (1997). "New spy law could cramp economy," *USA Today*, November 20, p15a.
- Slind-Flor, Victoria (1997). "New spy act to boost criminal defense Biz; Enhanced enforcement of trade secret theft expected," *National Law Journal*, April 28.
- Slind-Flor, Victoria (2000). "Industrial spying still flourishes," *National Law Journal*, March 29.  
[rhesq.com/CI/National%20Law%20Journal.pdf](http://rhesq.com/CI/National%20Law%20Journal.pdf)
- Superior Oil Co. v. State of Mississippi*, 50 S.Ct. 169 (1930).  
[www.charitableplanning.com/document/1386844](http://www.charitableplanning.com/document/1386844)
- Wexler, Michael; Milligan, Robert (2009). "Keeping on the right side of the line: A trade secret law perspective," *Competitive Intelligence Magazine*, V11n4 September/December p29-32.  
[www.scip.org/Publications/CIMArticleDetail.cfm?ItemNumber=10350](http://www.scip.org/Publications/CIMArticleDetail.cfm?ItemNumber=10350)

---

Richard Horowitz is an attorney concentrating in corporate, international, and security matters. He is the author of SCIP's Policy Analysis on Competitive Intelligence and the Economic Espionage Act, has advised SCIP on the revision of its Code of Ethics, and is a frequent speaker on the legal and ethical aspects of CI at SCIP conventions, local chapters, and other trade associations. His website is [www.rhesq.com](http://www.rhesq.com).