The Ethics of Competitive Intelligence: the Good, the Bad & the Gray

By Arik Johnson

To many, the term "ethical CI" seems to be an oxymoron, a lot like "jumbo shrimp". But, a more thorough exam of the professional literature reveals a broad spectrum of various competitive intelligence practices, including those that might be considered unethical by many.

Some CI references label any sort of ongoing surveillance as a questionable activity, while others argue we should be able to engage in certain forms of misrepresentation in order to gain information about a competitor, as long as the misrepresentation does not harm others by forcing them to participate in activities that violate their ethical duty. Because of these divergent viewpoints, it has been important that the profession develop its own sense of ethical guidelines that can be at once universal and also intuitively applied. Likewise, we can find guidance in corporate codes of conduct and make significant contributions to their ongoing development more broadly in the enterprise.

Especially in an era that produced the scandals of Enron, Worldcom and Arthur Andersen, we've all learned the need for our organizations to act with integrity, transparency and the good of the organization and its collective beneficiaries and stakeholders in mind at all times. But, there's a reason ethics are a philosophical pursuit. Because no matter how businesslike, questions of right and wrong are grounded in morality and worldview. Utilitarian, Kantian and Personal or Community Virtue ethics are frameworks that all play a role in crafting a set of ethical guidelines for the organization.

This is based on the ideas that, individuals given full disclosure will not interact knowingly with competing interests in a full and transparent manner, and incorporate the ideas that avoiding harm, while upholding both community and personal values, are good instinctive guidelines for everyone to follow in CI conduct. The requirements for full disclosure of identity, for example, in human intelligence collection are variously accepted or rejected by commission or omission depending upon who's doing the interviewing and what specific words come out in the conversation and how those words were elicited for extraction.

Even as some organizations are addressing CI ethics quite seriously, most CI practitioners find ethical policy-making a lonely job, relying on personal background and intuition as much as organizational policy to make tough ethical decisions. We're also trying to overcome the pressures and incentives pushing us to overstep our ethical boundaries, in violation of all the CI community holds dear. Finally, there remains a lack of consensus about the finer points - misrepresentation by omission being one of these; by the toughest of standards, it's considered unethical not to identify oneself fully under really any circumstances, even if not asked, specifically.

Does it happen then, that sometimes people break these guidelines? Of course, that's no surprise. There are even those who've said we're all guilty and have fallen short of the perfect standard, or

claim they're acting as whistleblowers for the CI profession at large, in telling the world what it is we're all "really up to". I have to disagree however with the notion that organizations more often than not willingly break ethical guidelines to get the tough business of CI done. If their general counsel knew of it, most organizations would disengage a third party caught misrepresenting themselves in order to extract information variables from a competitor. That said, if the policy is unknown throughout the enterprise and a part of its culture, what can people expect to occur in real application?

A lot of this misperception comes from the supposed influence of the American Intelligence Community on the development of the CI profession in what CIA, FBI, NSA or military intel personnel would call the "private sector". Patriotic or not, the image of the CIA is, at best, that of an organization with situational ethics so malleable as to be meaningless in the execution of its mission. But the differences are stark and the ends justifying the means require often life or death decision-making. And, while it may seem obvious, it's just not the same collection of outcomes or methods to arrive at a more secure country, as are applied in pursuit of a more competitive firm. This is where the most damaging cultural attachment with "espionage" derives; and it's not only untrue, but counterproductive to the profession.

All the above are mostly organizational cultural issues and culture can, over time, be molded to fit the needs of the environment in which an organization operates. Still, there are many high-profile lapses recently that point to the fact that culture is not enough. Many of these feed the "spy" and espionage hype that some in the CI business seem intent on promoting for personal gain.

Tens of millions of dollars in settlements and punishments have been meted out to some of the world's largest companies, across a range from VW/GM-Opel, Schwan's/Kraft-DiGiorno, P&G/Unilever, Boeing/Lockheed-Martin, Oracle/Microsoft, and the many books and other sources advocating questionable ethical standards, have made the business world at large wonder if CI is a trustworthy undertaking or even worth the risk. In a business where risk management is the core of what we do, it's contradictory for a board of directors to see it out in the development of an ends-justify-the-means group of spies.

The ongoing debate over the very words "competitive intelligence" is a source of frustration for many alternatives offered range from "decision support" to "early warning" to "competitive affairs" as viable alternatives, despite the obvious momentum CI as a designation has gained over the past 20-plus years of professional development, and its broader descriptive ability in capturing the more tactical aspects of the job.

SCIP, the Society of Competitive Intelligence Professionals, has done most of the defending of the profession in this regard, as well as having been a source of some hypocrisy among its own membership. There's a good reason for this: it is only ever possible to identify violators when laws are codified to govern behavior in any domain. SCIP's members, in joining the Society, agree to adhere to its multi-point Code of Ethics, which obliges them to gather information through legal and ethical activities, such as searching publicly available sources and conducting interviews in which they identify themselves and their employer.

But the Code also defines the standard by which accountability is determined, a standard often seen as too high for CI to be done effectively, or even in touch with reality as CI is practiced in the modern, global enterprise. The SCIP Code of Ethics remains however, the profession's equivalent of the "Ten Commandments" in terms of behavior:

- To continually strive to increase the recognition and respect of the profession.
- To comply with all applicable laws, domestic and international.
- 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 avoid conflicts of interest in fulfilling one's duties.
- To provide honest and realistic recommendations and conclusions in the execution of one's duties.
- To promote this code of ethics within one's company, with third-party contractors and within the entire profession.
- To faithfully adhere to and abide by one's company policies, objectives, and guidelines.

Indeed, anyone who knows SCIP also knows how seriously it takes the Code and the efforts made to educate members about ethical behavior. Unethical behavior is not only wrong and should not be condoned; it's bad for business.

One of SCIP's past board presidents commented, "the reported activities of a few bad apples who think of themselves as intelligence operatives (and who, incidentally, are not SCIP members) should no more discredit honest CI professionals than the sleazy actions by a few reporters should throw into doubt the integrity of all journalists."

Likewise, SCIP put in place a very conscious PR process to respond to any such connection between espionage and legitimate CI activities in recent years, even going so far as to suggest resignation for SCIP members in any way connected to such scandalous behavior wherever it's been hinted at.

Much of SCIP's codification is the result of the Economic Espionage Act of 1996, which, among other provisions, seeks to set out penalties and define violations of trade secrets under conditions of economic espionage. The full text of the section of the EEA96 is available from http://www.AuroraWDC.com/arj_cics_espact96.htm and sections 1831 and 1832 are detailed below:

1831. Economic Espionage

(a) IN GENERAL.--Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more others persons to commit any offense described in any of paragraphs (1) through (4), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years,or both.

(b) ORGANIZATIONS.--Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

1832. Theft of trade secrets

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate of foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more others persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

The conundrum then is that is the legal standard is quite a looser one, even though the outcomes of collection by ethical means might constitute the acquisition of trade secrets in violation of U.S. Federal law. This has always been a bone of contention - that, the means and ends of acquiring competitively advantageous knowledge of a rival's business plans, whether by inference or subterfuge is still codified as acquiring of a trade secret, in most cases. But, what is a trade secret, if that is the standard to which we must adhere in the legal realm, and is that enough or is it overkill in the ethical realm.

The important distinction in this argument is over the means of appropriation; mere possession or acquisition without fraud or misrepresentation as a means to that end is then allowed. For example, if a firm compiles the list of a competitors customers over time based on an understanding of which customers are lost in day-to-day sales activities after win/loss interviews with those customers determine whom was chosen as a functional equivalent, it can be inferred the identities and relationship details at a level of granularity approaching that which might be more speedily collected by unethical means - hacking into the competitors CRM system for example. A customer list acquired by the CRM hack is clearly unethical; a customer list acquired by legwork in diligently interviewing lost sales prospects, an equal outcome, is legitimate and allowed, that is, assuming those customers do not bread non-disclosure covenants otherwise in force with those competitors.

In order to define trade secrets, it's important to understand what the Federal law covers, and its jurisdiction outside the United States. To quote directly, "The term ‘trade secret’ means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing if, the owner thereof has taken reasonable measures to keep such information secret; and the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public."

Consider the case of General Motors' Opel division in Europe in the late 1980s which, following the sudden flight by GM's global purchasing czar, Jose Lopez de Arriortua, to Volkswagen, Opel

discovered he and his lieutenants had made off with critical purchasing and negotiating information about GM's component suppliers. After it became apparent that the "midnight file run" made by Lopez, VW's Ferdinand Peich eventually settled the matter out of court with GM/Opel - which included the transfer of a whopping $100 Million.

Frankly, before ethics became a major question in American business back in the 1980s, using subterfuge to "spy" on competitors was less of an issue. My father once described his interview for a sales job at a major furniture manufacturer early in his career. After a quick screening process, he learned they weren't interviewing for their own salespeople - they were looking for candidates that could get hired as salespeople by their competitors, with the ultimate goal to place knowledgeable "mole" employees in the competitor to funnel any and all useful information back to the company. Even though he'd always wondered what that would've been like, he admitted that he'd asked for the exit when he found out what he was actually going to be up to.

Ira Winkler, a former analyst with the National Security Agency, contends that American companies lose billions of dollars each year through preventable information leaks, most often those falling outside legal and ethical boundaries. In his 1997 book, Corporate Espionage, he shows how much of it is pilfered by unremarkable efforts - looking at memos, sifting through trash, peeking on desktops, or simply asking for it - and provides some advice to stop it. His day job is investigating industrial espionage, often testing company defenses by trying, usually successfully, to penetrate them in vulnerability assessments. The core of the book is a disguised case study, showing how Winkler was able to penetrate a corporation's computer network and records system.

In that process, he used many common, ethical and legal CI techniques to supplement or support the illicit ones. For example, he reviewed the target's annual report, press releases and even a company directory on its Web site, before making any contact with the target. The goal was to learn about the target's general organizational structure and environment, as well as to identify his own hit list of development projects, with the names of employees working on them. After reviewing these sources, he moved quickly to scanning Internet user groups and current magazine and newspaper articles. The results? He quickly came up with a list of the target's top six IT development projects, the names of several employees associated with one of those key projects; the office locations of these employees; and a good idea about the target firm's technical vulnerabilities in its firewall.

From here, Winkler moved into clearly unethical and often illegal "black" operations, using such tactics as: printing fake business cards which identified him as an employee with the firm's corporate security office; hacking into company computers using passwords freely given to him by duped employees; copying highly confidential files carelessly left on executive desks after hours and re-programming the company's terminal servers to allow him undetected off-site access. In three days, Winkler captured 250 megabytes of data while onsite, leaving 1,000 megabytes of "potentially useful data because I ran out of storage space" and totally compromised 28 of the company's top development programs. The value of the data to the target was estimated at over $1 Billion. Now, you know you've got a problem when the biggest

obstacle the penetration expert encounters is running out of storage for all the information they've just stolen from you.

The example above bears a clear absence of ethics in collecting competitively advantageous information. But, while codes of ethics make for good PR and often interesting reading, the lack of in-situ methods of mechanisms of monitoring code compliance or consequences of infraction of the organization's moral principles when transgressions occur, requires CI to take an active role in establishing enforcement and training committees to avoid future violations. This is especially important as CI permeates throughout the organization and becomes less of a centralized function - a process that is happening more and more - and increasingly part of everybody's job.

One opportune area for ethical lapses occurs with the entry interview process for new hires, especially those that used to work at competing firms, who now hope for whatever reason to contribute to the advantage of their new team on the field. Most people, if they're in knowledgeable roles with a prior employer, are subject to some either expressed or implied non-disclosure agreement governing proprietary information. Suggesting or inducing a new hire to violate that non-disclosure agreement is perilous at best and illegal at its worst. Every entry interview should begin with an examination of the NDA and questions in violation of the NDA should be avoided. Likewise, and perhaps more obviously, any and all documents in the possession of former competitor employees should be sent to the legal department, regardless of the presence of the words "confidential and proprietary" or not, where they will likely be returned to the competitor organization in as discreet a way as possible, without identifying the employee who bore them over the wall.

It's interesting that, as a third-party research collection and competitive analysis firm, we're often asked to do things that violate ethical CI practices. We're continually talking with first-project clients about how, "we have obtained a PowerPoint presentation, containing highly useful information, but which your general counsel would have a heart attack if it was known was inside your four walls". This explanation is almost always respected and appreciated, as guardians of the client's ongoing best interests and, to a certain extent, contributors to their ethical and moral true north on CI-related subjects.

It's also not surprising that certain "hungrier" competitors of our own willingly - often with great flair and salesmanship - solicit and accept such "hard-to-find" assignments that would, if the client's general counsel knew of their parameters, would likewise lead to a coronary in short order. Even conflicts of interest between third-party consultants and service providers should be explored, if not from a defensive perspective in protecting your own CI priorities and trade secrets accompanying them from unintentional disclosure to your own competitors, then at least to see whether the firm will ethically accept the assignment from you, knowing full well they have an existing relationship with a another conflicting client in the same marketplace. The conflict standards in the advertising business are obvious and strict; in CI, they must be no less severe.

My own views on the matter of such client conflicts seem to disagree with so much of new-client opinion governing the paramount value of so-called "industry experience" by whichever firm is ultimately hired, over more general domain expertise and adaptable skills, which I find much more important. A good example is the pharmaceuticals industry, where it's not uncommon for what are in effect bribes to be paid to knowledgeable sources on research subjects sought by consultants, at a rate sometimes as high as thousands of dollars per hour! In this case, industry experience amounts to little more than knowing how big an "honorarium" to pay, not what the scientific background looks like.

Likewise, conflict of interest dynamics usually dictate that a firm that has done work in a particular therapeutic area for a competitor in the past 12 months is off-limits; but in a system of "hungry" service providers, self-regulation of these requirements is often pointlessly self-selective. History tells us that, most ethical lapses are caused, not by the company's own CI staff, but by third-party contractors playing fast and loose with the system, lying and misrepresenting themselves not only to their clients' competitors, but often to the clients themselves. This is a cultural phenomenon at play more broadly in our society and applying higher ethical standards is difficult at best. But as a community, it's important to network the knowledge of those that live in "bad neighborhoods" so that they can be avoided and ultimately leave the field.

I hope I've answered the question of whether the term "ethical CI" is an oxymoron. Not only is ethical CI possible, it's necessary for a firm to remain competitive. But unless fundamental guidelines are followed, the otherwise high-reward value CI can return to the firm remains fraught with risk in the collection of the information variables required to be done exhaustively. Sticking to my own three-part "Golden Rule" is my best parting advice: if it would embarrass the organization if your behavior were reported on the front page of tomorrow's newspaper, it's a bad idea; if your own company would find that behavior on the part of a competitor unethical and take legal action against the offending organzation, it's a bad idea; and, finally, my favorite, if you think your mother would punish you for it, then it's definitely a bad idea.

In the final evaluation, it's interesting to look back at the actual examples of costly ethical transgressions and see that CI as a profession was almost completely absent from and unaware of these activities. However, as we move from the modern, explicit CI functional team into a networked, implicit sense of CI that permeates the organization at large, it becomes part of the competitive intelligence mission to be an evangelist of standards and clearinghouse of best practices on the ethics of competitive advantage. Business is not war, because the ends are far different; in applying intelligence techniques then to business, the means of arriving at competitively advantageous ends must also be different.

Whatever course an organization takes in building and developing a CI function and staff, it must first apply its values to the mission statement and means by which CI will accomplish its primary task: to enhance the market position of the firm relative to its competitors in the eyes of its customers.

Failing that mission, CI is of no use to anyone.

Aurora WDC | 520 West Grand Avenue | Chippewa Falls, WI 54729 | USA
www.AuroraWDC.com | +01.715.720.1616 | ReconG2@AuroraWDC.com

Arik Johnson

Phone: +01-715-720-1616
Email: arik.johnson@aurorawdc.com

Aurora Staff Biography: Arik R. Johnson

Arik R. Johnson is Founder, Managing Director and CEO of **Aurora WDC**, Senior Fellow of the CI **Best Practices Institute** and Chief Strategist of Aurora's **Research & Analysis Bureau**, where he advises business leaders seeking greater understanding, systems for early warning, risk management and predictability about their competitive environment, market rivals and customer behavior.

Arik is author, architect and curator of Aurora's internationally acclaimed **ReconG2 KnowlegeBase** (www.ReconG2.com) of CI tactics and strategy. Arik's staff of consultants applies cutting-edge methods from Aurora's Best Practice Institute in the field laboratory of the Research & Analysis Bureau to benefit a diverse clientele in creating sustainable competitive advantage with Aurora as a virtual member of their CI team and support personnel.

Before Aurora's launch in 1995, Arik was a business analyst and advisor with a leading international management-consulting firm after earning degrees from the University of Wisconsin-Madison in Business, History, Political Science and International Affairs.

Arik also speaks and teaches worldwide to audiences on the intersection of subjects of interest to him ranging from market research, competitor analysis, customer relationship management, strategic planning and knowledge management to software, politics, psychology and journalism.

Arik writes a daily online "Weblog" journal critiquing business events and competitive strategy called "***Competitive Intelligence***" (www.AuroraWDC.com/ci), is editor and publisher of Aurora's weekly "***Recon CI News***" (www.ReconCI.com) with more than 15,000 subscribers worldwide, and is also a contributing editor or columnist to various periodicals on business competitiveness topics, including *KMWorld* and SCIP's *Competitive Intelligence Magazine* (www.SCIP.org).

Arik is chairman emeritus of SCIP's Wisconsin chapter and today serves on SCIP's Board of Directors and is winner of SCIP's 2005 Catalyst Award for his legacy of contributions to the Society. Arik is a sought-after and popular speaker at CI-related events around the world, having delivered more than 600 lectures, keynotes and workshops on CI throughout his career in venues across the Americas, Europe, Asia-Pacific and Africa.

Alongside traveling and spending time with his wife Tina and son Liam (and cats, Luther and Phoebe), Arik volunteers as a mentor to young people in leadership and entrepreneur programs, as well as giving pro bono consulting advice to small businesses and charities in and around his Wisconsin countryside community of Chippewa Falls, while serving in advisory roles to many corporate, government and education organizations.

For answers to questions or advice on developing competitive intelligence tools and techniques as part of your organization's market strategy, contact Arik anytime by email at Arik.Johnson@AuroraWDC.com, or through Aurora WDC in the U.S. or Canada by calling 1-800-924-4249 or +01-715-720-1616 worldwide.

Aurora WDC | 520 West Grand Avenue | Chippewa Falls, WI 54729 | USA
www.AuroraWDC.com | +01.715.720.1616 | ReconG2@AuroraWDC.com