Webology, Volume 8, Number 2, December, 2011

The new competitive intelligence agents: "Programming" competitive intelligence ethics into corporate cultures

Emilie Steele Giustozzi
M.S.K.M., College of Continuing Education, University of Oklahoma, 1700 Asp Avenue, Norman Oklahoma 73072, Tel: (405) 325-7161. Email: esteele (at) ou.edu

Betsy Van der Veer Martens
Ph.D., Knowledge Management Program, University of Oklahoma, Schusterman Center, 4502 East 41st Street, Tulsa, Oklahoma 74135, Tel: (918) 660-3376. E-mail: bvmartens (at) ou.edu

Received September 30, 2011; Accepted December 9, 2011

Abstract

This article examines some of the ethical issues involved in competitive intelligence activities on the Internet. We discuss the importance of an ethical framework for the performance of competitive intelligence, especially the Code of Ethics of SCIP (the leading professional association for strategic and competitive professionals), in the context of today's networked global environment. The virtual borderlines separating national economic and military territories online are becoming increasingly hard to determine, and a variety of intelligence activities now impact organizations of every size. We describe how competitive intelligence is often practiced by employees and firms with no clear understanding of the legal and public relations problems that various ill-advised initiatives may create for both individuals and the organization, inasmuch as the Internet greatly facilitates the use of sophisticated software products without correspondingly sophisticated ethical perspectives. Specifically, we offer two mundane and seemingly minor examples of how the uninformed use of microtasking software such as Field Agent and identity misrepresentation software such as Persona Management may actually be detrimental to the existence of an ethical organizational culture. We concludes by offering suggestions as to how to help employees "program" themselves into being effective and ethical CI "agents" for their organizations.

Keywords

Astroturfing; Competitive intelligence; Ethics; Field agent; Mystery shopping; Persona Management; Strategic & Competitive Intelligence Professionals (SCIP)

Introduction

Every business leader knows the truism that business success is the ability to provide the right product to the right market at the right time for the right price. Achieving these goals in today's highly competitive marketplace requires sound leadership, strategic vision, and a firm understanding of the competition. As such, the field of competitive intelligence (CI) has become vital to organizational success (Rittenburg, Valentine & Faircloth, 2007). CI practitioners seek out information about the competition and create organizational knowledge to support managers and leaders in their decision-making. As a curious blend of ancient military strategies (Cantrell, 2003) and contemporary marketing research techniques (Walle, 1999), CI's focus is broader than just the realm of advertising and market share. Rather, an "understanding [of] the strategies, capabilities, and options" (Walle, 1999, p. 519) of others in the industry can influence decisions throughout an organization. Businesses of any size may benefit from undertaking CI projects, but must be careful to understand the ethical considerations surrounding such work, especially in today's global information environment.

As both corporate and nation-state information technologies become more globally connected and, thus, more accessible to competing needs for what Luhn (1958) dubbed "actionable intelligence," the shifting lines between civilian and military environments continue to blur (Eeells & Nehemkis, 1984; Knapp & Boulton, 2006). Cyberwarfare can now take place on both the economic and military fronts of any nation, and it is becoming increasingly difficult to distinguish whether it may be a country or a competitor behind any given instance of "industrial espionage." Recent examples in the news run the gamut from Dupont's winning of a $920 million lawsuit against South Korean competitor Kolon for the theft of trade secrets involving Dupont's Kevlar body armor (Valk, 2011), to the hoax perpetuated on French car-maker Renault, which led the automotive company to accuse China of suborning some of its managers, finally resulting in public apologies and financial recompense to the accused by Renault (Reed & Thompson, 2011); to the out-of-court settlement between Motorola and its Chinese competitor Huawei regarding the "leakage" of intellectual property belonging to both firms (Cheng & Raice, 2011).

While the companies involved in newsworthy CI scandals tend to be large in size and international in scope, these are also the companies that have had the opportunity to create compliance policies and invest in formal CI. Organizations like these are compelled by legal and industry expectations to have such governance controls in place. Companies that do not have organized programs or interest in CI from their leadership may find themselves both victims of and vulnerable to similar problems related to information gathering and use. However, most attention has been focused towards managing the information security risks (e.g., Fowler, 2011) rather than the ethical risks (e.g., Fleming & Zyglidopoulos, 2008). Similarly, most attention to the ethical issues of corporate online activities tends to focus on those involving customers (e.g., Bush, Bush & Orr, 2010; Roman, 2010) rather than competitors.

While it can be argued that every company today should have leaders who understand business information issues, including those related to CI, small and start-up businesses are seldom in a position to cultivate such knowledge. But, as a company grows, the needs for strategic planning and for controls spike at the same time that responsibilities and tasks must be distributed (Churchill & Lewis, 1983, p. 42). Employees, therefore, must take on new organizational information-processing roles as the company becomes "a knowing organization" (Choo, 2006) and be made aware that their online responsibilities can impact the reputation management of their firm, both positively and negatively (Tennie, Frith & Frith, 2010; Fiedler, 2011). Just as employees should be informed upon entry into the organization that their at-work email behaviors must conform to company guidelines, they must be made aware of the implications of and temptations offered by globally networked information seeking. This becomes increasingly important as companies employ a more diverse workforce, representing a wider range of ages, backgrounds, and sociotechnological proclivities (Myers & Sadaghiani, 2010).

Existing Ethical Guidelines

Before exploring the challenges awaiting organizations developing and maintaining a CI program, it is important to understand what kinds of guidance are available in this field. Codes of ethics are lists of rules intended to promote good behavior (Kaptein & Schwartz, 2008). Codes written by professional organizations are closely associated with the associated field, but only members of such organizations are obligated to uphold them. The code of ethics of the leading professional organization for CI, the Strategic and Competitive Intelligence Professionals (SCIP), forms the bedrock of any discussion of CI ethics. This code reads as follows:

- 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 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. (Strategic & Competitive Intelligence Professionals, n.d.).

These seven points are straightforward in theory, and yet they can be vague in practice. Honesty, adhering to law, and following company policies are obviously good guidance for behavior, yet Trevino and Weaver (1997) point out that there are times when the law is unclear, and companies may try to push employees past their ethical boundaries. To add even more confusion, what is legal in one country may be illegal in another (Rittenburg, Valentine & Faircloth, 2007). SCIP's code does not guide practitioners in weighing such facts in particular situations, but appears better suited to introducing ethical boundaries to those new to the field.

Of course, as the SCIP Code of Ethics notes, companies often have their own codes of ethics and other governance policies. Fehringer & Hohhof (2006) collected 22 of these to allow practitioners to see the range and depth of the field. Some are short, providing minimal elaborations on SCIP's code, while others go into more detail and even provide specific guidelines for behavior. Fuld and Company's ethical policies start with the procedure for identifying oneself at the beginning of a phone call, thus providing clear expectations on how to uphold SCIP's third point regarding the disclosure of identity. SCIP's wording does not define how much information must be given. Fuld and Company clarifies this for its employees: "Begin telephone calls by asking your question. When asked to identify yourself, give your full name. If also asked where you are calling from, state 'Fuld and Company,' …" (Fehringer & Hohhof, 2006, p. 154). Studying these policies can help CI practitioners understand what the expectations are within the professional community.

Practitioners grappling with real-world situations can also turn to other ethical models. For instance, Laczniak & Murphy (1991, p. 264) present four rules of thumb to guide marketing professionals:

- The Golden Rule–act in a way that you would expect others to act toward you.
- The Professional Ethic–take only actions that would be viewed as proper by an objective panel of your professional colleagues.
- Kant's Categorical Imperative–act in a way such that action taken under the circumstances could be a universal law of behavior for everyone facing those same circumstances.

- The TV Test–a manager should always ask, would I feel comfortable explaining this action on TV to the general public?

Charters (2001) developed a similar model specifically for the field of CI. The CHIP model is comprised of four factors: Community Virtues, Harm, Individual as End, and Personal Virtues. Like Laczniak and Murphy's rules of thumb, each factor is related to a different context in which to view a troublesome action. Unsurprisingly, given that marketing and CI have much in common, the models are so similar that Charters' Community Virtues factor maps to the Professional Ethic and the TV Test, Personal Virtues maps to the Golden Rule, and the Categorical Imperative maps to Individual as End. Where Charters's model differs is his focus on the evaluation of the cost vs. the benefit of an action and on his consideration of individuals with whom the CI practitioner interacts. The Harm factor is based in utilitarian ethics in which the consequences of an action determine its ethical quality, i.e., the ends justify the means. This factor considers whether the product of the action is worth more than the harm caused by the action. There are some situations, however, in which no amount of benefit should outweigh the harm caused to another. To avoid such actions, CHIP uses a different wording of Kant's Categorical Imperative: "all humanity should be treated as an end and never as a means only" (Charters, 2001, p. 48). This humanizes others with whom a practitioner may come into contact or conflict.

Neither of these models is comprehensive in scope, but they both serve to guide practitioners in reflecting on specific situations. While the practitioner is still left to decide what to do, these models provide some rubrics for considering the underlying ethical issues.

Hazards in the Road

The literature reveals three challenges to companies creating and implementing programs to encourage ethical behavior in CI programs. First, the most well documented code of ethics for the field belongs to SCIP. However, CI tasks are often undertaken by those who do not consider themselves CI practitioners (Ng Kwet Shin & Spence, 2002; Marin & Poulter, 2004). This opens organizations up to unintentional bad behavior by those who do not realize they are engaging in CI. Second, ethical behavior is often tied to codes of ethics and other behavioral codes. While studies of the efficacy of ethical codes are inconclusive, some evidence exists that such codes are of limited use lower in organizational hierarchies (Nyberg, 2008). Third, technology and business practices normally develop faster than formal codes of ethics or laws, creating wide gray areas for practitioners to wander through with limited guidance (Rittenburg, Valentine & Faircloth, 2007).

Challenge 1: Who Does CI?

When CI first began to emerge as a profession in the 1960s, gathering intelligence was a full-time task, requiring highly developed skills and resources (Wilensky, 1967). Finding the right information is still a skill that must be refined and practiced, but the Internet has ushered in a new age in information access. Information requests that may have once taken days or even weeks to complete can often now be accomplished with a quick search engine query or with the ongoing use of a computer algorithm on a company's web site. The software programmers who develop these algorithms, moreover, often have little or no contact with those who make use of these algorithms for their own purposes. The Internet also allows CI consulting companies to market directly to managers, potentially sidestepping in-house CI staff. These issues cause problems in understanding who actually performs CI functions within organizations. Marin & Poulter's (2004) survey of SCIP members highlights the diversity of positions in which employees identify as CI practitioners. Of their ten possible job labels, only one, "Lone CI manager" was defined as exclusively related to CI (p. 197). Of the respondents, only 18% felt that label described their position.

Unlike the members of SCIP, not everyone who participates in CI identifies such tasks as belonging to a particular profession. For instance, a manager who is curious about operations within a competitor's store may commission a "mystery shopping" study from a consulting firm. Mystery shopping is commonly used by businesses to evaluate their own customer service performance; however, the practice is also used to evaluate competitors and monitor their sales practices. In such a situation, a person from the firm would pose as a customer to the competitor. In this scenario, the manager would not necessarily see this as part of CI work. Rather, in a company that does not discuss CI, he or she could easily consider this information collection as just part of his or her strategic planning process. Without knowledge of CI as a field, the manager cannot evaluate whether the consultants are acting in an ethical fashion, thus opening up the company to potential problems.

Mystery shopping itself is an ethical sticking point. Yes, it is commonplace and legal, but the mystery shopper is not forthcoming with his or her identity or purpose, which seems to conflict with the third point in SCIP's code of ethics. In studying this conflict, Ng Kwet Shin & Spence (2002) interviewed managers who commission mystery shopping studies, sales associates who have been mystery shopped, and a professional mystery shopper dedicated to CI information collection. They also recognized that mystery shopping is often conducted by student workers or consultants, distancing employees from the actual act of deception. Their results showed little concern amongst anyone involved about the ethics of collecting information from competitors. Indeed, since "mystery shopping" can be accomplished online by the utilization of software agents ("shopbots" and "pricebots") without any direct human supervision, it can be viewed as a purely technical exercise in data collection (Desouza, 2001). Thus, those who commission and participate in online or offline mystery shopping may not consider possible backlash from competitors or customers.

Challenge 2: Deciphering the Code

Since employees may not be aware of SCIP or their own participation in the CI field, companies need to address ethics as a broader issue within their organizations. One way they may do this is by implementing a company-wide code of ethics with sub-codes as needed. Nyberg recognizes that the consequence of various business scandals has been the development of such ethical codes (2008, p. 587). Organizational codes of ethics have been shown by some studies to influence ethical behavior positively (e.g., Adams, Tashchian & Shore, 2001), but the literature is by no means conclusive on the subject (Kaptein & Schwartz, 2008, p. 114). The success of ethical codes relies on such rules applying universally (Clegg, Kornberger & Rhodes, 2007, p. 109). Yet in practice, ethical codes are not always clear, and real-world CI activities can be complex.

Despite the implementation of many well-intentioned codes of ethics, Nyberg (2008) found that employees lower in an organization's hierarchy are less influenced by formal codes as they are by practical wisdom. While codes are useful tools for leaders and managers evaluating business decisions and employee performance, employees find themselves making practical decisions in situations in which a code of ethics is but one of many influences. In realistic situations, ethical considerations are weighed against competing concerns like performance metrics, time, convenience, and personal investment. In practice, pressure from a manager who wants efficiency even at the expense of customer service will eventually wear down an employee's personal dedication to the customer (Nyberg, 2008, p. 594).

Kaptein & Schwartz's (2008) model of business code effectiveness supports Nyberg's findings. In their model, the content of a business code is filtered through its implementation by corporate leadership, the organizational culture, and the character of the employees themselves. Leaders who implement these codes are much closer to their content than other employees. And yet it is the actual behavior of front-line employees that create the largest effect for the organization, not the codes themselves (p. 118). Due to such limitations, company leaders cannot assume that the adoption of an organizational code of ethics will result in ethical behavior throughout the workforce. Ethical compliance by employees needs to be regularly scrutinized as part of any performance review.

Challenge 3: Technological Temptations

Internet communication is known for its ability to elicit bad behavior from otherwise "good" people. Such behavior can include harassment (Davis, 2002) and piracy (Lysonski & Durvasula, 2008). Dehumanization of those on the other end of Internet-based interactions can cause people to fail to recognize situations in which they would otherwise follow a moral or ethical rule when interacting directly with a person (Alnuaimi, Robert & Maruping, 2010). The anonymity provided by screen names and online communication can psychologically separate people from their actions, which can relieve Internet users of their sense of responsibility (Johnson, 1997). Further, as Boyd (2007) points out, as the use of avatars and personas become increasingly common in personal online life, the boundaries between personal and professional lives become even more problematic. The automatic deployment of arrays of so-called "intelligent agents" to collect information online can further separate any inappropriate actions from the responsible parties (Kwon & Sadeh, 2004).

Such new technology often exposes organizations to unexpected problems. Those writing ethical guidelines even 15 years ago could not have fathomed the amount of previously private information made public through the Internet, the widespread computing power, nor the vulnerability of many information systems to internal and external intrusion, both covert and overt. Nevertheless, the problems that arise from these developments can be seen as permutations on existing issues. Paine (1991, pp. 426-249) recognized four indicators of unethical behavior in CI activities: misrepresentation, improper influence, covert surveillance, and unsolicited intelligence. New dangers from digital technology can be placed in these categories as readily as the hazards of a more analog age.

Misrepresentation can be as simple as someone giving the wrong name in a conversation or as complex as submitting a bid as a non-existent vendor to a competitor in order to investigate their internal environment. But in any real-world deception, the utmost care must be given to maintain the lie. Phones must be answered with the correct name. Letters must go out on the right stationery. The truth must be kept separate from the fiction. These little particulars are often the ones that are forgotten, unraveling the entire scheme. Many see the Internet as a place full of lies and untrustworthy interactions (Johnson, 1997), but those with skills and time can often find the holes in such fabrications as well. For instance, email headers can provide a plethora of identifying information, IP addresses can reveal a user's location, and an identity's lack of backup references across open information sources can signal that it is a fake. Just as in real life, the devil is in the details.

However, the development of so-called "Persona Management" software by HB Gary Federal reportedly allows even an average user to manage multiple personas from one computer with much greater ease and effectiveness (Rockefeller, 2011). In this case, a "persona" is an artificial identity, complete with email and web site accounts, convincing web references, and other content meant to prove that this person is "real." This software would handle the crafting of otherwise identifying information, like IP addresses, to conform to the requirements for a specific identity, and failure points of manually-managed fake personas (i.e., sending an email from the wrong email address) would be mistake-proofed with features like visual cues to remind users of the persona as whom they are acting.

This technology can be used to create the artificial appearance of popular support for an idea, product, or candidate, a practice called "astroturfing" (so named because it involves the creation of an artificial illusion of "grass-roots" support). Lee (2010) recognizes this as an extension of marketing techniques going back to the early 20th century. Nevertheless, astroturfing is recognized as unethical amongst the marketing community and has been linked to damage to the corporate image when discovered. Astroturf posts to blog comment threads and forums are marked by an unnaturally positive attitude toward a product and an overreliance on links to marketing web sites (Cox, Martinez & Quinlan, 2008). Regular users have often been able to recognize such insincere participation, but Persona Management makes detection more difficult. As this software was designed specifically to facilitate mass deception by government agencies, critics are already deeply concerned about it (Anderson, 2011). The strong nexus between military and business intelligence research and development technologies has become even stronger in recent years, as the military solicits civilian firms to create a variety of intelligence software applications and then eventually transfers the resulting technology back into the civilian sector for use (Mowery, 2009). Persona Management software and similar products are very likely to find non-military markets as well.

This practice causes problems for CI professionals on two fronts. First, blogs, forums, and other social media are open information sources which can be mined to study the public's perception of a company or its competitors. Astroturfing contaminates these resources and any analyses based on them. While this is a hindrance to data collection, CI practitioners may also be tempted to use Persona Management software to pose as competitors' customers, business partners, job applicants, etc. This would clearly be in violation of SCIP's Code of Ethics, but the factors associated with anonymity and dehumanization may make such practices almost irresistible unless specifically prohibited.

Technology can also be used to conduct covert surveillance. This type of ethical violation need not be associated with obvious spying technology like bugs or hacking. Ethical issues can arise from seemingly unrelated technology as well. Amazon.com's Mechanical Turk service is a microtask site in which workers are given small tasks to complete. These tasks are generally difficult to process by computer, i.e. dictation, categorization, proofreading, etc., leading to the site being dubbed "Artificial Artificial Intelligence" (Amazon, 2012). This refers to the fact that from a company's perspective, they enter a task into the computer interface, and later, results come back. Yet in reality, the job has been broken down into its component tasks and completed by workers who are unaware of the goal of the work or others who are working on it. Various other microtask sites have emerged since Mechanical Turk's introduction in 2005, but a company called Field Agent (2011) has a new spin on the model. Whereas older microtask companies rely on computers, Field Agent is an iPhone app, allowing for tasks that require workers to go to a specified location to complete. "Retail intelligence" is one of the named uses by clients on the Field Agent web site.

In a previous section, the challenges presented by the large CI consulting industry were identified as a problem for managers unaware of CI or its associated ethical considerations. Microtask companies pose similar problems, though the influence of technology may make bad behavior alluring even for CI practitioners. Microtask platforms are best suited for time-consuming and repetitive tasks. There are a variety of CI gathering tasks that fall into these categories. Online mystery shopping is one such example, bringing with it all the ethical baggage associated with its real-world counterpart. Another example that takes advantage of Field Agent's mobility would be a hypothetical task that asked a worker to take a picture at a certain place and time within a competitor's store. Whereas it would not be feasible to send an employee or contractor to monitor a competitor's deployment of cashiers throughout a week, both for cost concerns and the possibility of raising suspicion on the part of the competitor, mobile microtasks make this type of data collection possible.

While these examples of possible uses of microtasking for CI are relatively ethically tame, the anonymous nature of such systems makes users vulnerable to bad behavior. There are documented instances of CI practitioners using contractors to do work that would go against CI ethical obligations (Fitzpatrick, 2003). Microtask platforms add another layer of distance between the practitioner and the action–the platform is a faceless computer interface and the contractors are completely anonymous. The backlash by the public for an egregious covert surveillance campaign using microtasking could potentially be more severe than other outcries over ethically questionable behavior because of this use of members of the public.

Recommendations

We have outlined a variety of ethical challenges that may await unwary businesses. Small and growing businesses would no doubt find such a list daunting. Nonetheless, despite the differences in these problems, their root causes can all be addressed by two actions: 1) the dissemination of information regarding the field of competitive intelligence, and 2) the promotion of ethical cultures within businesses. Both of these solutions are within reach of any interested organization and, ultimately, will provide more than just protection from harm.

SCIP's Code of Ethics' first point, "to continually strive to increase the recognition and respect of the profession," can seem self-serving at first reading. Ethically obligating its members to tell others about it is definitely a good marketing strategy. However, the point is made for a much more important reason. CI is relatively unknown as a profession outside of business management. As such, laypeople are unable to recognize actions that are part of this profession. Anyone could tell you that heart surgery is a medical procedure and that only a doctor should perform it. By educating employees about CI, leaders can help avoid problems arising from CI activities being completed and contracted by employees who are unfamiliar with the field. Such discussions can also help remind CI practitioners about the ethical boundaries of their field so that they are not seduced by new opportunities offered by technology.

The development of an ethical culture within an organization is not a simple task, however. As Challenge 2 showed, ethical codes are not enough to develop an ethical culture, though they are often the first step. Trevino and Weaver (1997) found that the ethical culture of an organization, or lack thereof, had an effect on the behavior of CI practitioners. Those who worked for companies with a compromised ethical culture reported a willingness to bend ethical guidelines because they felt it was expected of them. However, those who perceived ethics as being important to the organization took their ethical obligations more seriously.

Ethical codes are important to the formation of ethical cultures because they provide the basis for beginning the discussion. Leaders can continue to promote ethical behavior by doing the following:

- Making ethical compliance part of employees' performance review (Fitzpatrick, 2003)–Clearly stating expectations for ethical behavior as part of the job description sets expectations before problems arise.

- Encouraging upper management to commit in word and action to ethical behavior (Trevino & Weaver, 1997)–Not only is it important to set a good example, but employees who can trust their leaders feel safe enough to stand by personal principle when faced with external pressures.
- Providing opportunities for discussion and training based on practical application of ethical guidelines (Nyberg, 2008)–As highlighted by Challenge 2, ethical codes are meant to be universal and, thus, necessarily vague. Therefore, employees need practice applying ethical guidelines to real-life situations. Also, by opening lines of communication on the topic, ethics become a topic for ordinary conversation, not a stressful discussion initiated only in a crisis. Just as the biggest threat from competitors is the unknown, competitive intelligence is only dangerous when it is left unexamined and misunderstood. By discussing the role of competitive intelligence with employees and promoting an ethical culture throughout the organization, firms of any size can help their employees "program" themselves as CI agents capable of operating successfully and ethically in any environment they may enter.

References

- Adams, J.S., Tashchian, A., & Shore, T.H. (2011). Codes of ethics as signals for ethical behavior. *Journal of Business Ethics*, 29(3), 199-211.
- Alnuaimi, O.A., Robert, L.P., & Maruping, L.M. (2010). Team size, dispersion, and social loafing in technology-supported teams: A perspective on the theory of moral disengagement. *Journal of Management Information Systems*, 27(1), 203-230.
- Amazon. (2012). Welcome. *Amazon Mechanical Turk*. Retrieved September 30, 2011, from https://www.mturk.com/mturk/welcome
- Anderson, N. (2011). Black ops: How HBGary wrote backdoors for the government. *Ars Technica*, February 2011. Retrieved September 30, 2011, from http://arstechnica.com/tech-policy/news/2011/02/black-ops-how-hbgary-wrote-backdoors-and-rootkits-for-the-government.ars/
- Boyd, D. (2007). None of this is real: Identity and participation in Friendster. In Kasraganis, J. (Ed.), *Structures of Participation in Digital Culture*. (pp. 132-157). New York: Social Science Research Council.
- Bush, V., Bush, A.J., & Orr, L. (2010). Monitoring the ethical use of sales technology: An exploratory field investigation. *Journal of Business Ethics*, 95(2), 239-257.
- Cantrell, R.L. (2003). *Understanding Sun Tzu on the art of war*. Arlington VA: Center for Advantage.
- Charters, D. (2001). The challenge of completely ethical CI and the CHIP model. *Competitive Intelligence Review*, 12(3), 45-54.
- Cheng, R., & Raice, S. (2011). Huawei, Motorola strike a truce in dueling lawsuits over patents. *Wall Street Journal*, (April 14, 2011), B3.
- Choo, C.W. (2006). *The knowing organization: How organizations use information to construct meaning, create knowledge, and make decisions*. 2nd ed. New York: Oxford University Press.
- Churchill, N.C., & Lewis, V. L. (1983). The five stages of small business growth. *Harvard Business Review*, (May-June, 1983), 30-50.
- Clegg, S., Kornberger, M., & Rhodes, C. (2007). Business ethics as practice. *British Journal of Management*, 18(2), 107-122.
- Cox, J.L., Martinez, E.R., & Quinlan, K.B. (2008). Blogs and the corporation: Managing the risk, reaping the benefits. *Journal of Business Strategy*, 29(3), 4-12.
- Davis, J.P. (2002). *The experience of 'bad' behavior in online social spaces: A survey of online users*. White paper. Social Computing Group. Microsoft Research.

Retrieved January 21, 2012 from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.84.5025

- Desouza, K.C. (2001). Intelligent agents for competitive intelligence: Survey of applications. *Competitive Intelligence Review*, 12(4), 57-63.
- Eells, R., & Nehemkis, P. (1984). *Corporate intelligence and espionage: A blueprint for executive decision making*. New York: Macmillan.
- Fehringer, D., & Hohhof, B. (Eds). 2006. *Competitive intelligence ethics: Navigating the gray zone*. Alexandria, VA: Competitive Intelligence Foundation.
- Fiedler, L. (2011). Reputation management in different stakeholder groups. In Helm, S. et al. (Eds.), *Reputation management: Management for professionals*. (pp. 127-149). Berlin: Springer-Verlag.
- Field Agent. (2011). Agent FAQ. *Field Agent*. Retrieved September 30, 2011, from http://www.fieldagent.net/agent/agentFAQ/
- Fitzpatrick, W. (2003). Uncovering trade secrets: The legal and ethical conundrum of creative competitive intelligence. *SAM Advanced Management Journal*, 68(3), 4-13.
- Fleming, P., & Zyglidopoulos, S.C. (2008). The escalation of deception in organizations. *Journal of Business Ethics*, 81(4), 837-850.
- Fowler, G. (2011). What's a company's biggest security risk? You!: Employees don't mean to be a primary entry point for hackers - but they are. *Wall Street Journal*, (Sept. 26, 2011), 3.
- Johnson, D.G. (1997). Ethics online. *Communications of the ACM*, 40(1), 60-65.
- Kaptein, M., & Schwartz, M.S. (2008). The effectiveness of business codes: A critical examination of existing studies and the development of an integrated research model. *Journal of Business Ethics*, 77(2), 111-127.
- Knapp, K.J., & Boulton, W.R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management*, 23(2), 76-87.
- Kwon, O.B., & Sadeh, N. (2004). Applying case-based reasoning and multi-agent intelligent system to context-aware comparative shopping. *Decision Support Systems*, 37(2), 199-213.
- Laczniak, G.R., & Murphy, P.E. (1991). Fostering ethical marketing decisions. *Journal of Business Ethics*, 10(4), 259-271.
- Lee, C.W. (2010). The roots of astroturfing. *Context*, 9(1), 73-75.
- Luhn, H.P. (1958). A business intelligence system. *IBM Journal*, 2(4), 314-319.
- Lysonski, S., & Durvasula, S. (2008). Digital piracy of MP3s: Consumer and ethical predispositions. *Journal of Consumer Marketing*, 25(3), 167-178.
- Marin, J., & Poulter, A. (2004). Dissemination of competitive intelligence. *Journal of Information Science*, 30(2), 193-208.
- Mowery, D.C. (2009). National security and national innovation systems. *The Journal of Technology Transfer*, 34(5), 455-473.
- Myers, K.K., & Sadaghiani, K. (2010). Millennials in the workplace: A communication perspective on millennials' organizational relationships and performance. *Journal of Business and Psychology*, 25(2), 225-238.
- Ng Kwet Shing, M., & Spence, L.J. (2002). Investigating the limits of competitive intelligence gathering: Is mystery shopping ethical? *Business Ethics: A European Review*, 11(4), 343-353.
- Nyberg, D. (2008). The morality of everyday activities: Not the right, but the good thing to do. *Journal of Business Ethics*, 81(3), 587-598.
- Paine, L.S. (1991). Corporate policy and the ethics of competitor intelligence gathering. *Journal of Business Ethics*, 10(6), 423-436.
- Reed, J., & Thompson, J. (2011). Renault apologises over false spy claims. *Financial Times*, London (UK), (March 15, 2011), p. 15.

- Rockefeller, H. (2011). Updated: the HB Gary email that should concern us all. *Daily Kos*, February 16, 2011. Retrieved September 30, 2011, from http://www.dailykos.com/story/2011/02/16/945768/-UPDATED:-The-HB-Gary-Email-That-Should-Concern-Us-All
- Rittenburg, T.L., Valentine, S.R., & Faircloth, J.B. (2007). An ethical decision-making framework for competitor intelligence gathering. *Journal of Business Ethics*, 70(3), 235-245.
- Roman, S. (2010). Relational consequences of perceived deception in online shopping: The moderating roles of type of product, consumer's attitude toward the internet and consumer's demographics. *Journal of Business Ethics*, 95(3), 373-391.
- Strategic & Competitive Intelligence Professionals. (n.d.). *SCIP code of ethics for CI professionals*. SCIP (Strategic & Competitive Intelligence Professionals). Retrieved September 30, 2011, from http://www.scip.org/About/content.cfm?ItemNumber=578
- Tennie, C., Frith, U., & Frith, C.D. (2010). Reputation management in the age of the world-wide web. *Trends in Cognitive Sciences*, 14(11), 482-488.
- Trevino, L.K., & Weaver, G. R. (1997). Ethical issues in competitive intelligence practice: Consensus, conflicts, and challenges. *Competitive Intelligence Review*, 8(1). Retrieved September 30, 2011, from http://osint.pbworks.com/f/Trevino.pdf
- Valk, V. (2011). DuPont wins $920 million in Kevlar trade secrets case. *Chemical Week*, 173(23), (September 19- 26, 2011), 9.
- Walle, A.H. (1999). From marketing research to competitive intelligence: Useful generalization or loss of focus? *Management Decision*, 37(6), 519-525.
- Wilensky, H.L. (1967). *Organizational intelligence: Knowledge and policy in government and industry*. New York: Basic Books.

Bibliographic information of this paper for citing:

Giustozzi, Emilie Steele, & Van der Veer Martens, Betsy (2011). "The new competitive intelligence agents: "Programming" competitive intelligence ethics into corporate cultures." *Webology*, 8(2), Article 88. Available at: http://www.webology.org/2011/v8n2/a88.html