THE PERSISTENCE OF A STIGMATISED PRACTICE: A STUDY OF COMPETITIVE INTELLIGENCE

Patrick Reinmoeller
Cranfield School of Management
Cranfield University
Cranfield, Bedford MK43 0AL
United Kingdom
Tel: 44 (0) 1234 751122; Fax: 44 (0) 1223 751806
patrick.reinmoeller@cranfield.ac.uk

Shaz Ansari,
Judge Business School
University of Cambridge
Cambridge, CB2 1AG
United Kingdom
Phone: +44 1223 768 128
Fax: +44 1223 339701
Email: s.ansari@jbs.cam.ac.uk

Accepted for publication in British Journal of Management

THE PERSISTENCE OF A STIGMATISED PRACTICE: A STUDY OF COMPETITIVE INTELLIGENCE

ABSTRACT

Studies on the diffusion of practices provide valuable insights into how organisations adopt, adapt, sustain and abandon practices over time. However, few studies focus on how stigmatised practices diffuse and persist, even when they risk tainting the adopters. To address this issue and understand how firms manage stigmatized practices, we study U.S. organisations associated with the practice of competitive intelligence (CI) between 1985 and 2012. CI includes legitimate information gathering practices that are sometimes also associated with infringements and espionage. Our findings suggest that CI became highly diffused and persisted despite the risk of stigmatising its adopters. We identified three factors to explain CI's persistence: 1) keeping it opaque to avoid the negative effects of stigmatisation, 2) "constructing" usefulness to justify its ongoing use by leveraging accepted beliefs and invoking fear of unilateral abandonment and 3) adapting it by developing multiple versions to increase its zone of acceptability. These three factors contribute to practice persistence by allowing firms to dilute the potential stigma from use of the practice. Our contribution lies in explaining the adoption, diffusion and ongoing use of a stigmatised practice whose benefits cannot be overtly acknowledged nor made public.

Key words: Diffusion, practices, adoption, adaptation, practices, management fashion, legitimacy, stigma, competitive intelligence

INTRODUCTION

Practices such as golden parachutes for CEOs of failing banks and executive bonuses are now widely criticised, but endure and are even supported by taxpayers' money to keep banks solvent. While abundant research has examined how controversial industries arise (Baum and McGahan, 2013; Humphreys, 2010) and polemic practices diffuse (Briscoe and Murphy, 2012; Davis and Greve, 1997), scant research has addressed their persistence (Colyvas and Jonsson, 2011). For practices to persist they need to be perceived as either adding technical or social value; they "do good" or "look good" (Kennedy and Fiss, 2009). Some widely diffused and clearly legitimate practices, such as advertising, consulting, and external hiring persist in light of perceived commercial gains, even if sometimes questionable (e.g., Bidwell, 2011; Sturdy, 2011; Verhoef and Leeflang, 2009). Some legal practices, such as downsizing (Ahmadjian and Robinson, 2001), golden parachutes (Fiss, Kennedy and Davis, 2012), and retiree benefit cuts (Briscoe and Murphy, 2012) persist because of commercial benefits, even if they do not look good. Illegal practices such as deceptive accounting, price-fixing, environmental degradation (Greve, Palmer and Pozner, 2010), sweatshop labour (Lamin and Zaheer, 2012), bribery (Martin *et al*., 2007), paying protection money (Vaccaro and Palazzo, 2014) and modern day slavery (Crane, 2013) put adopters at risk of stigma (Jonsson, Greve and Fujiwara-Greve, 2009), but continue because of commercial gains, even if these gains need to be hidden. It is worth exploring how and why risky stigmatised practices persist when

their benefits cannot be overtly acknowledged or made publicly visible.

A prominent exemplar of a stigmatised practice that persists is competitive intelligence (CI). Based on the assumption that "high-quality intelligence is, on balance, desirable" (Wilensky, 1967: xi), CI refers to legal practices of gathering market information that have sometimes been associated with legal infringements and espionage (e.g., Calof and Wright, 2008). Nearly every major firm has a CI office designed to gather market information and/or to discover the "trade secrets of competitors." CI practitioners operate in virtually every form of enterprise, including non-profits (Nasheri, 2005: 9; King and Bravin, 2000a). CI has diffused[i] and persists, despite patchy evidence of competitive gains[ii] (Richardson and Luchsinger, 2007; Saayman *et al*., 2008) and reputational risk from its illegal deployment (espionage).

Given limited research on stigmatised practices (cf., Crane, 2005; Hemphill, 2002), we examine how CI has evolved, diffused and persisted. We identify three factors to explain CI's persistence. First, keeping a practice opaque may allow a stigmatised practice to persist. Due to reputational and financial risks, users justify keeping CI "under the radar." Second, since adopters and other stakeholders cannot overtly show performance benefits to justify utility and ongoing use, they construct usefulness by leveraging accepted beliefs or "endoxa," (Green, Li and Nohria, 2009, p. 14; Wilensky, 1967), and by invoking fear about the risks of unilateral abandonment. Third, they adapt the practice by developing multiple versions,

thereby increasing the "zone of acceptability." These three factors contribute to practice persistence by allowing firms to dilute the potential stigma from using the practice.

We contribute to the literature on controversial practices in three ways. First, while much research has focused on the diffusion of practices, we extend the limited number of studies on practice persistence (Colyvas and Jonsson, 2011; Zhu and Westphal, 2011). Second, we explain the diffusion and persistence of stigmatised practices whose commercial benefits need to be actively kept opaque to avoid reputational risks and how firms justify its ongoing use beyond just rhetorical defence (e.g., Carberry and King, 2012; Elsbach and Sutton, 1992). Third, we shed light on a practice associated with intelligence studies that has received scant attention in organisation theory, despite absorbing considerable resources without overt benefits (Grey, 2009).

THEORETICAL MOTIVATIONS

In explaining practice adoption and persistence, scholars have moved beyond conceptualising institutional and technical forces of adoption as separate and distinct (Ansari, Fiss and Zajac, 2010; Greve, 1995; Tolbert and Zucker, 1983; Westphal, Gulati and Shortell, 1997) by emphasising the social embeddedness of technical factors (e.g., Kennedy and Fiss, 2009; Lounsbury, 2007). Once practices diffuse organisations seek either technical or social benefits, if not both, accruing from continued implementation. At times, practices persist despite questionable technical benefits (e.g., Abrahamson, 1991); the accounting practice of

managing gross margins in agriculture persists because it is simple, popular, and largely unchallenged even by those in the know (Jack, 2005). Similarly, Soin and Huber (2012) show how a meta-form of financial regulation has persisted over time in UK retail financial services despite lacking systematic evidence of benefits.

At times, new controversial practices may diffuse and persist despite social disapproval because organisations strategize to deflect criticism or defend against potential stigmatisation (Desai, 2011). Practices may also persist because organisations proclaim to engage in legitimate versions of the practice, or dissociate themselves from scandal-prone firms. An example is mixed martial arts, where practitioners have distanced themselves from more extreme versions of the practice (Helms and Patterson, 2014). Similarly, firms in the arms industry straddle multiple categories to dilute their association with the stigmatized category (Vergne, 2012). Organisations may also be able to "insulate" themselves from institutional pressures against controversial practices, which explains why modern day slavery still persists (Crane, 2013).

Clearly, stigmatised practice may continue because adopters are attracted by commercial gains, such as cheap labour in the case of modern day slavery, or lucrative loyal fans in the case of violent sports. Yet, the degree of stigma varies. In the case of violent sports, commercial gains can be made public, but for modern day slavery, these gains need to be kept hidden. The literature on impression management , i.e., "tactics designed to affect the

perceptions of the image, identity, or reputation of an organization" (Elsbach, 2006, p. xvii), offers insights into rhetorical strategies (e.g., Elsbach & Sutton, 1992), defensive mechanisms (Carberry and King, 2012; Desai, 2011), and the use of dominant positions in a field to dampen criticism and deflect stigmatisation (Jonsson and Buhr, 2011). However, we still need to learn more about how firms defend their ongoing use of stigmatised practices whose benefits need to be kept subliminal and how they find ways to manage the potential stigma that may arise from engaging in these practices.

COMPETITIVE INTELLIGENCE: GATHERING INFORMATION OR SPYING?

Over the last two decades, CI has diffused dramatically (Green, 1998; Javers, 2010; Rogers and Ruppersberger, 2012; Teitelbaum, 1992). See Appendix 1 for quotes from media references on CI and its widespread use. CI is defined as "the collection of information, internal, external and from competitors, but also from customers, suppliers, technologies, environments, and potential business to provide early warning and help to predict the moves of competitors, customers, and governments" (Calof and Wright, 2008: 723; Gilad, 1996). All professional activities to gather digital and non-digital information are subsumed under CI (SCIP, 2013; Bose 2008) that is associated with a range of practices (e.g., Fair, 1966; Hirsch and Levin, 1999) spanning from legal gathering of market information to infringements of the law and corporate spying (Nasheri, 2005).

Investigating rivals and industrial espionage is clearly *not* the same thing. While "CI is

gathering information on rivals through legitimate means, such as published data and interviews" (Curtis, 2001: 28), open source data (Fleisher, 2008; Pikas, 2005), "text mining, web mining and visualisation-based CI tools" (Bose, 2008: 510), "[s]pying is the grubby business of spying, bin-sifting and office-bugging, often illegal and always unethical" (Curtis, 2001: 28). "Techniques range from quizzing the company's employees and benchmarking a competitor's products to surfing the Internet, lurking around industry trade shows, and even rooting through rivals' rubbish bins" (Armstrong et al., 2009: 115) and employing "cyber sleuths" (The Economist, 2013a).

Thus, while gathering and analysing strategic information is a legitimate practice, the way information is gathered and treated can lead rivals, clients and others to suspect even legal CI activities (Cohen, 2013; Dodd, 2013; Holmes, 2013). Using CI can be risky as even a single firm's illegal espionage activities that transgress ethical and legal boundaries can also vilify legal CI by other firms (cf., Jonsson et al., 2009). Yet, despite frequent revelations of espionage and scandals, information leaks and moles, which further stigmatise CI, the practice is seldom evaluated systematically by organisations or society in general. Although professional publications often exhort the need for more spending on CI to gain competitive advantage (e.g., Choo, 1998; Fuld, 1995; Wilson, 2001), knowledge on CI remains limited (e.g., Davison, 2001; Ghoshal and Westney, 1991), anecdotal (Rogers and Ruppersberger, 2012), specialised (e.g., Hannula and Pirttimaki, 2003), or application oriented (e.g., Nolan,

1999; Swartz, 2005).

Indeed, "in the modern, competitive business world, millions are spent on CI information gathering" and "discovering the truth" (Nasheri, 2005: 77) and the "largely hidden industry is becoming an integral part of the way companies do business around the world." Industry insiders fear that the intelligence industry "can expect tougher rules" following a rising number of scandals and the industry is "just one scandal away from a government crackdown" "with so much unsavoury conduct going on" (Javers, 2010: xii). Yet despite the risks, firms continue in engage in both legal and illegal forms of CI. And, even when they gain from its legal use, the benefits of CI use often need to be kept well hidden. Thus examining CI provides a promising opportunity to analyse how stigmatised practices persist when their perceived benefits are difficult to demonstrate.

METHOD

CI attracts large investments that are not being accounted for.[iii] Finding an appropriate setting for CI was challenging as detailed information on CI is not included in commonly used financial databases such as Thompson One Banker or company publications, such as annual reports, which include expenses on R&D and Marketing & Sales but not on CI costs. The limitations to access data on CI were partly overcome by using the digitally available public record of CI activities and the role of media in exposing deviant firms (Jonsson and Buhr, 2011; Desai, 2011) to select polar or "extreme cases" (e.g., Eisenhardt and Graebner, 2007) in

terms of a company's association with CI (See Appendix 2). Seeking large companies with media exposure, we formulated our sample from companies that stayed in the Fortune 500 and the S&P 1200 from 1985 to 2005 (310 companies from 41 industries). We used two main data sources. First, as reporting on CI is relatively sparse,[iv] we conducted a longitudinal analysis of archival data on CI use across industries and organisations. We relied on academic papers, annual reports and news releases, papers from regulatory agencies and trade associations (e.g., Jones, 2002) and posts on dedicated websites (e.g., www.asis.org). Second, we gathered qualitative data mainly from semi-structured interviews lasting 30-90 minutes with 14 experienced CI practitioners – providers and clients of CI services including former and current CEOs and directors in the companies we selected. Interview transcriptions totalled 184 pages. Examples of questions include: "What benefits and downsides of CI do you see?" and "Could you describe how investments in CI are justified?" No questions alluded to illegal activities but these were noted in informants' discussions of CI activities. We promised confidentiality to encourage cooperation and candour (Glick *et al*., 1990; Huber and Power, 1985). We addressed potential subject bias by employing multiple data sources (Jick, 1979). Table 1 lists the interviewees and Table 2 lists the case companies.

----------Insert Table 1 and Table 2 about here ----------

Our case selection process consisted of six steps. *First*, we analysed how firms competing in different industries are associated with CI. We developed a list of keywords to capture the

media attention CI received from 1985 to 2005 in the 41 industries to which our companies belong. We identified extreme cases in terms of CI association, i.e. mention of CI in industry and firm "in order to more easily observe contrasting patterns in the data". For fair comparison, we employed a single source (Wall Street Journal) and used the same set of keywords to capture firm data. *Second*, we analysed how firms in industries with the strongest CI association, Business Services and Electronic Equipment, compared with firms with the weakest CI association, Fast Moving Consumer Goods. Using the same set of keywords, we gained an overview of CI in these industries` firms from 1985 to 2005. *Third*, our purposeful sampling allowed us to choose polar types in which the process of interest is "transparently observable" (Eisenhardt, 1989: 537). This led to the selection of four polar organisations in each of the two high (total of 8 firms – IBM, Unisys, Intel, Linear Technology, Microsoft, Motorola, Oracle, Texas Instruments) and one low CI industries (total of 2 firms - Unilever and Procter & Gamble). Thus in total, we studied *ten* firms; (Table 2.1, 2.2. 2.3 and 2.4). *Fourth*, using additional key words (e.g., CEO, top management, IT, organisations, and procedures) we drew on six data sources to write short company cases on the ten case companies covering the period 1985-2012.[v]

---------Insert Tables 2.1, 2.2, 2.3 and 2.4 here--------

We sought evidence on the evolution of CI and also included primary data on these companies. We conducted a cross-case analysis following Gioia et al.'s (2010) approach and

identified emerging commonalities (Table 3.1-3.2) along events, actors, practices, processes, and structures. Tables 3.1-3.4 summarise the development of CI in the ten organisations from the 1980s to 2012[vi].

---------Insert Table 3.1, 3.2, 3.3 and 3.4 here--------

Fifth, identifying links with CI along events, actors, practices, processes, and structures and iterating between data and theory, led to the emergence of five themes from which we distilled three factors that contributed to or detracted from persistence (Table 4.1-4.2).

----------Insert Table 4.1 and 4.2 about here ----------

CI's EMERGENCE AND PERSISTENCE

Using archival and interview data, we tracked the emergence of CI within and across our selected organisations, its methods of deployment including centralisation and formalisation, and damage control in light of misconduct. We explain how CI emerged, diffused, and persisted illustrating the findings with quotes from our interviewees and the media.

CI's Emergence and Initial Diffusion Our analysis showed variation in CI's use across industries. Besides being enabled by resource allocation to intelligence functions (Wilensky, 1967), CI often emerged following crises (Table 2.3-2.4) and a sense of victimisation (Tables 2.1, 2.3-2.4). After Motorola adopted CI (Table 2.2; 3.1), five firms launched CI initiatives in the late 1980s. CI was often adopted based on expected gains despite experiences with often illegal CI. Finding allies in media and regulatory bodies, victimised firms challenged CIs

legitimacy, only to subsequently engage in it. For example, P&G received $125 million for the violation of its rights but later engaged in CI (Table 2.3; 3.1). Similarly, after IBM became a victim of espionage, it developed its own CI routines and later turned it into a business line (Table 2.1; 3.1). Not engaging in CI was considered "too risky" an IBM expert noted. CI practices also emerged from industry recipes shared by organisational leaders. "Why CI? Greater minds than I have decided to do it, so I do it." (Manager 12, Oracle) CI adoption ranged from hiring contractors (e.g., Motorola in 2.2) to creating internally dedicated units (e.g., IBM in 2.1; 3.1). The boundary between legitimate and illegitimate CI versions was not always clear.

After initial adoption prior to or in the 1980s, the media showed how large organisations started using CI, e.g., at IBM (Table 3.1) and Texas Instruments (TI) (Table 3.2), where CI first targeted technology, or at Unisys where suppliers became involved (2.4; 3.2). The scale and scope of CI practices, as covered by media, appears to gradually increase with its perceived inevitability (Table 3.1-3.2). However, media visibility created a dilemma. Although it was important to increase CI's *internal* visibility for intra-firm knowledge sharing, this also increased external visibility that risked company reputation. Across cases, the strong involvement of CEOs and top management increase both internal and external visibility. Our data indicates widespread adoption of CI by 2000. The emphasis shifted to CI as a business opportunity (Table 3.1-3.2). Interviewees noted CI's diffusion, the use of CI

portals, guidelines for acceptable conduct, and opaqueness of the central CI function.

> "…there is a practitioner portal where you can get information. This is a huge pot of information. You get all these tools but no-one really tells you what's best. You have to find out on your own." (Manager 1, IBM)

> "I really have no idea how this portal functions" (Manager 11, Oracle)

The dilemma becomes apparent when scandals erupt. For example, P&G's leaders were associated with questionable CI activities of one of their service providers. Admitting involvement, they agreed to a $10 million settlement to avert court proceedings (Nelson and Ellison, 2001). Similarly, Oracle's CEO was questioned about investigators acting on his behalf, whose transgressions were exposed by the media (Hemphill, 2002) (Tables 2.3; 3.1). We also found indications of decentralisation, which reduced the internal and external visibility of CI at Microsoft (Table 3.1) and Unisys (Table 3.2). However, reducing internal visibility limited CI's usefulness, as intelligence could not be shared freely in the organisation. Our CI experts also reported questionable CI activities by external CI providers.

> "Our partners, let's say our resellers… are more resourceful in digging up information. The quality of that information is sometimes very good, but sometimes it's also a problem." (Manager 4, IBM)

> "If you're really using insider information for financial gains in the equity market, you can get arrested and that's bad. But I think that corporate espionage is much harder to prove. I think some CI activities are valuable and fairly risk free." (Manager 12, Oracle)

CI's Formalisation and Standardisation

Users and providers across all companies clearly believed in CI's utility and inevitability in keeping rivals at bay with claims like: "It's important to know…" (Manager 11, Oracle) and

"It's all about the information you have…" (Manager 3, IBM). We find that CI was standardised across companies by hiring external professionals, and in some cases, even the same main experts. These experts merged consulting and training practices, registered the tagline "the gold standard in CI education" (ACI, 2014) and had half of the companies on the Fortune 500 list as clients. This reflected CI practitioners' alignment on the means, goals and constraints of CI usage (Tables 2.1-2.4; 3.1-3.2). The diffusion of CI as an "acceptable" industry practice in a competitive market tends to largely eliminate differential effects at the firm level. One CI expert explained:

> *"*Basically, we follow who they are, what they do …this is quite critical to us. So we really aim for, they call it black on white, hurting [competitor A], [competitor B]… wherever we can. Therefore, we want to know where they are, how they sell, how they operate. So, we want to find their weak spots, to understand them, to really breathe the oxygen that our competitors breathe, and understand what drives them." (Manager 2, IBM)

> "You want to be able to give the ammunition to your sales force…they can email [to a specific website] and someone specialised in this specific product area can give them support, contents and ammunition." (Manager 9, Microsoft)

CI can lead to competitive parity. With every player knowing more about the other, the level of transparency in an industry may rise and the value of information for one firm may decline (Whitney and Gaisford, 1999). For example, competitors hired the same consultants, or each other's executives (Table 3.1- 3.2) and CI analysts "traded information with counterparts in competitor organisations and third-parties" (Jaworski, Macinnis and Kohli, 2002: 289). CI providers and clients acknowledged these "open secrets".

> "There are scientific organisations like IEEE, they arrange conferences where people present some of their findings. …they all know each other. They went to university

together. They know about each other's work…. It is a fairly small community" (Manager 7, Intel)

An ex-Unilever employee noted that Unilever and P&G – "two of the most advanced users of CI" (Curtis, 2001: 29) – engaged in similar CI activities, and frequently reached the same conclusions. Similarly, the bitter rivalry among UK's supermarkets often led to similar tactics. "We'd do all the usual stuff, such as sending staff shopping in competitors' stores, getting them to check on promotions, and asking questions to the customer services manager" (Curtis, 2001: 29). Standardisation could thus cancel out firm-level differential advantages.

Transgressions and Reputational Damage from the use of CI

The practice still remains largely hidden from outsiders and is often revealed through scandals. CI clearly carried reputational risks in the companies we examined (Table 3.1-3.2) and its legitimacy was openly challenged in courts (Tables 2.1-2.4). After it was revealed that the activities of Oracle's supplier of CI services had engaged in "dumpster diving" (searching for information in target's trash), its reputation and share price suffered (Stone, 2000). In many cases, companies continued the practice despite involvement in CI scandals, either as perpetrators or victims (e.g., IBM, Microsoft, Oracle, P&G, TI and Unilever). Corporate scandals around spying suggest that CI was often seen as illegitimate, and its proponents needed to conceal its use, or justify it as "building defences" against intruding rivals (Jameson, 2011; Wilson 2001). Our cross-case comparison shows how transgressions often marked the beginning of CI engagement, made it appear inevitable and led to further

investment in the practice. Our interviewees reported that fierce rivalry justified CI despite the risks. The choice is often seen as "binary".

> "I make sure they lose the game…there's no second place. You either win or you're lost." (Manager 12, Oracle)

> "You can't afford not do to this. In my company…you can't afford not to keep up. It's very tough, very competitive and it's like a sprint race all the time." (Manager 10, Motorola)

Concern for reputational damage was shared by several CI experts:

> "Because [company] is one of the biggest, it's always among the first to be sued. We're always seen to be liable because we've got big pockets." (Manager 2, IBM)

> "We had to pay hefty fines after competition court declared [our company] guilty in the past. In order to avoid that, we spend a lot of money trying to avoid getting caught again." (Manager 14, Unilever)

While scandals reverberated in the media, numerous cases were settled out of court resulting in multi-million dollar payments (See Tables 2.1-2.4; 3.1-3.2). Across our cases we find considerable consistency in CI victims settling out of court. Firms engaging in CI after victimisation knew about the costs suffered by exposed perpetrators of illegal and illegitimate CI. Yet they still chose to engage in risky CI activities:

> "There have been quite a few lawsuits between IBM, Microsoft, EMC, and a number of all the big players where these sort of legal cases have attracted a lot of publicity. Ultimately they're all settled, in some financial way." (Manager 10, Motorola)

> "Yes, we take some risk. Basically, we think it's a good story, or we heard it's good stuff, so we fall for it and try it. We set aside a quarter of the budget for some of that stuff, but really we never know whether it's valuable information or not. But it sounds good, so we try it." (Manager 4, IBM)

Crises and appeals for the right to legitimate defence can lead to further investments to make effective and keep legal what in the past has been proven to be risky.

> "Rather than having problems with our competitors, we spend money to avoid trespassing the law. We're spending more money in training our people not to violate competition law than training our people in knowing what our competition is doing … because of potential violations, and unfortunately in the past that was the case." (Manager 14, Unilever)

Interview findings match press accounts where CI scandals have led to arrests and falls in company share prices (Moffett and Pearson, 2011). While admitting to "failings and dysfunction" within Renault, the CEO vowed to fight competitive disinformation (The Economist, 2011). Even defensive measures to protect company secrets from competitors (Javers, 2010) can be seen as intrusive by employees, or suppliers obliged to follow their clients' security rules (Wilensky, 1967) (Tables 2.1-2.4; 3.1.-3.2). When CI is associated with moles, spies, and information theft that make headlines, CI's legitimacy becomes moot.

Diversification of CI and Damage Control

The "hidden industry of spies for hire" (Javers, 2010: xi) thrives without much scrutiny (e.g., King and Bravin, 2000a; 2000b) through diversification and damage control. Practices accepted in some contexts may be seen as suspect in other contexts (Wright and Roy, 1999).

> ""Here, let me show you" And you could see his laptop on the screen, and he said "This is what we did at my old company". He had the specs…the recipe of what they had done at his previous company. And our guys went "No, no, no, no! Turn it off… you can't have that here. You gotta take it off your computer.…. Delete it. We don't do that at [company]. …we can't do that here." That basically set the tone that we aren't going to allow it. But it's bit of a dilemma, because it's tempting, right?" (Manager 7, Intel)

Transgressions are often settled out of court (Tables 2.1-2.4); and by removing the key individuals involved (e.g., Table 2.3) to avert public scrutiny. The 1996 Economic Espionage Act put firms engaging in CI transgressions at risk of criminal prosecution (Javers, 2010). Ten

years later, only a few cases have been brought to court, many involving sting operations by the FBI (Nasheri, 2005). Yet, companies continue to engage in risky CI practices.

EXPLAINING PRACTICE PERSISTENCE

Our empirical analysis and building on extant theory revealed three factors to explain how companies are able to persist with a stigmatised practice. Keeping the practice opaque averts or mitigates the negative effects of stigmatisation, constructing usefulness creates positive reasons for continuation, and adaptation allows differentiating and legitimating one's own practice version from the stigmatised category.

Creating opaqueness to conceal use of the practice

We find that the lack of transparency and observability of CI activities – tried and tested mostly in classified use at the national level and among a community of professionals[vii] – preclude objective assessment (cf., Rogers, 1995) and leads to persistence. CI experts find that protecting CI activities requires keeping them secret or opaque.

> "[T]he strategy of protecting our intelligence is to keep it secret as long as possible…And then, all of a sudden, we released a new product and…we would say "by the way we're using this technology" and everybody in the industry was kind of surprised. Now they have to catch up and that'll probably take them…even if they can see our [products]… 4 years at least to figure out how to do it." (Manager 7, Intel)

> "[Company] has never hired people from their competitors ....we don't trust them. They could be a double agent. We could hire people from a competitor, train them for four or five years, and they could quit and go back to the original competitor and take everything with them." (Manager 6, Intel)

> "Our vendors are not allowed to see the recipes on the machines. In many cases, they still own the machine but they can't see what we're doing to it. So, there's this balance of "hey

> we need your help to fix this problem", but we won't tell them what we are doing because we don't want them to know. And they will go like: "Well, we can't fix the problem because we don't know what you are doing." So, it's kind of a weird co-ownership of the machinery." (Manager 7, Intel)

Collectively, the industry seeks to avoid assessment about ongoing use of CI that spreads like an "open secret" (Taussig, 1999). CI is not overtly advertised, internally or externally. The opaque nature of the practice and its deployment (Dufresne and Offstein, 2008; Jones, 2008) impedes external assessment, while the manner of gaining access to hard to obtain strategic information also hinders internal assessment. CI often has a low profile in a company, making it difficult for organisations to find and utilise CI or to gauge its effectiveness. We found different views on the perceived risks and advantages of CI.

> "We get blinded by it… it's sometimes really time consuming...and maybe we shouldn't spend so much time on it. Also, getting good quality is difficult." (Manager 2, IBM)

Respondents also noted keeping only top management informed in the organisation:

> "Usually these reports are only for people in higher levels of the organisation. For me, in my business, I know much more than what the CI team knows…but we don't communicate much" (Manager 13, P&G)

While increasing risks, the use of external CI contractors further decreases transparency, as seen in the cases of Oracle/Microsoft and Unilever/P&G (Table 2.2-2.4). A CI expert noted:

> "I don't know how [contractors] do it all but a lot of it is via the Internet. ... We pay for these. I experienced situations, more like, "how did you get this" "this has become illegal". It is really beyond…" (Manager 3, IBM)

Keeping the practice relatively inconspicuous allows it to diffuse "under the radar". Hiring experts from "secret services" (e.g., IBM, see Tables 3.1-3.2), developing strategic alliances with intelligence firms funded by the CIA (e.g., Unisys, see Tables 2.4; 3.2), and using outside

contractors (e.g., Oracle), also keep CI invisible, except for those *in the know*. We failed to find transparent accounting and budgeting for the practice (e.g., "We don't keep track of [CI] activities" (Manager 11, Oracle)). It is commonly included in accounts that do not carry legitimacy risks such as market research or R&D and thus allows users to claim that CI entails relatively low levels of investments. "Mostly it's part of the marketing budget" (Manager 10, Motorola). Companies maintain CI departments and allocate substantial resources to CI activities without having to account for it or report associated gains:

> "If a senior executive says "Thou shalt do CI" – well then there's your return on investment, do it or lose your job. The benefits may not be quantifiable but it's job or no job." (Manager 12, Oracle)

Through concealed use, an organisation "adopts a practice and actively hides this adoption from external players" (Terlaak and Gong, 2008: 855) to 1) build barriers to imitation 2) limit reputation damaging leakages and 3) insulate the company against market pressures to report commercial gains. Yet resources for keeping the practice "secret" may dwindle as the practice diffuses. While diffusion may make concealing more difficult and attaining competitive advantage less likely, organisations have a collective interest in keeping the practice opaque.

> "I'm really not comfortable with my inputs on that portal. So, I don't actually give inputs to CI, I use it." (Manager 11, Oracle)

> "Personally, I try to keep that secret, right. It's an advantage." (Manager 1, IBM)

Wilensky (1967) showed how once documents are categorized as classified, the relative share of "secret" communication increases. Safeguarding secrets can bestow "specialness" on the clique of their guardians (Herman, 1996). As people attribute more value to what is

classified, they derive a "higher status" from handling it and being privy to it, and avoid divulging details to outsiders. This dynamic may collectively enable persistence.

Constructing Usefulness of the Practice

Ideologies, doctrines or beliefs about means and goal appropriateness (Wilensky, 1967) strongly influence firms' CI management. A former CEO of Motorola stated: "Intelligence, in my estimation, cannot simply be derived from your traditional business practices" (Galvin, 1997: 3). Such webs of beliefs or "endoxa" can permit actors to make a virtue out of secrecy (Green, Li and Nohria, 2009), and pre-empt challenges or questions. Where CI activities often involve retaliatory measures by CI's victims to "get even", the practice is still rooted in the belief that "hard-to-access" knowledge about what other organisation know, plan and do, is potentially useful and valuable information and worth accessing (Costas and Grey, 2014; Herman, 1996), despite the risks. Likewise, the conviction that more information reduces uncertainty increases the willingness to continue investing in CI (Wilensky, 1967).

> "You have to keep up with your competitors – otherwise you'll find yourself lagging behind new developments. If the industry changes you can find yourself, you know, 4 years behind; it's really difficult to catch up…that is a downside, I guess, of NOT doing competitive intelligence." (Manager 7, Intel)

The perception that all information, not publicly available or disclosed, has to be valuable (Costas and Grey, 2011; Dufresne and Offstein, 2008), and thus worth uncovering can precede and sustain both legal and illegal CI practices.

Even if amassing intelligence is shown to be of limited effectiveness (Howard, 2011), our

analysis suggests the belief that intelligence is key to staying ahead of rivals remains resilient. A respondent noted CI's historical link to commercial success at Motorola (Table 2.2, 3.2), despite CI's role in preparing Iridium – one of the biggest investment failures in technology infrastructure in modern times. Breaking with standard industry practice creates perceived risks arising from unilateral abandonment. This dynamic is similar to what is seen in arms races (Wallensteen and Sollenberg, 1996). Just as firms face social pressures to climb bandwagons, they also face pressures not to jump off them until a threshold number of firms do so, creating "safety in numbers" (Ahmadjian and Robinson, 2001). Our analysis also revealed the role of fear. In our interviews, CI experts noted that creating fear, uncertainty and doubt (FUD) was meant to "hurt" competition.

> ""Find me dirt". We call it battle cards. Battle cards are pieces of collateral we gave to the sales force that they could use in competitive situations. ... We would get our sales people to tell FUD stories: fear, uncertainty and doubt. This was a big thing...We had a counter FUD....I didn't have to say anything. I created FUD. That was enough to shift them to my side." (Manager 12, Oracle)

McKenna (1996) suggests that "entrepreneurs have pervasive fears of being victimised; they are continually scanning their environment for something to confirm their suspicions"...If we look hard enough there is always, somewhere, some confirmation" (Kets de Vries, 1989: 160-161). Fear and competitive threats makes it difficult to abandon CI (cf., Kieser, 1997). As game theorists e.g., Schelling (2007) argued in the analysis of the outbreak of World War I, the fear of being unprepared against a ready adversary greatly diminishes the perceived range of effective options (Ahlstrom, Lamond and Ding, 2009). Even the symbolic invocation of

fear can reinforce the collective belief to continue with a controversial practice. In the case of CI, managers may feel "assaulted by competitive change and fear" that they cannot "effectively channel and apply vital intelligence" (Fuld and Borska, 1995: 21). Victims are often reluctant to report incidents, as they "hesitate to acknowledge their negligence and do not wish to decrease the confidence level of clients or shareholders." These "fears also explain why it is so difficult to find real cases in which organisations are identified" that could clarify CI's consequences (Wright and Roy, 1999: 55). CI victims feel like they have no choice.

> "As a victim of CI you have to be very careful. You can't label another company as the perpetrator without proof. This could have legal consequences." (Manager 1, IBM)

By drawing on ideologies and invoking fear, actors can make a virtue out of secrecy. As long as these beliefs about usefulness are collectively nurtured within teams, firms, industries, or communities, practices rooted in these beliefs can persist. A particular organisation is unlikely to discard a highly diffused practice that has become a rationalised myth (Meyer and Rowan, 1977), even if it risks generating negative stakeholder judgments.

Adapting the Practice

Certain practices may persist because they lend themselves to multiple interpretations and can be adapted to multiple agendas (Benders and van Veen, 2001). In contrast to more contractually formalised practices such as franchising, protected by patents or legal stipulations (Godfrey *et al*., 2012), CI encompasses a broad range of practices, some less stigmatised than others. Practices with questionable legitimacy may persist because

organisations modify them to increase their zone of acceptability (Ansari *et al*., 2010), or positively position their own legal version of the practice. A CI expert noted[viii].

> "I mean as long as it's legal. [Company] is very strict about following the law whether accounting or anywhere else. So, as long as it's legal, I don't think that anyone has ever been concerned about gathering intelligence. (Manager 6, Intel)

Transformations in strategic planning at General Electric (GE) to facilitate changes in corporate agendas and management styles allowed strategic planning to persist (Ocasio and Joseph, 2008). Although CI has reached a high level of standardisation, we identified several modifications in its usage which has made it more inclusive and acceptable.

Our analysis suggested two adaptations that has allowed CI to persist; one to avoid legitimacy crises and the other to survive them (cf., Desai, 2011). CI is opaque, which allows it to stay under the radar. However, when scandals erupt, the CI community is quick to engage in "impression management" and to reemphasise the legitimate aspects of gathering intelligence.[ix] Strong commitment and even direct involvement of top management can portray CI as an activity associated with legitimate "knowledge management".

Also, the community sides with the press in condemning the few "bad guys", and shadowy contractors involved in CI as belonging to the netherworld of intelligence. Transgressors are occasionally made scapegoats and provided as "fodder for the press," in the words of a practitioner (Manager 1, IBM), to distinguish them from CI professionals (Table 2.3).

Corporations may also try to diffuse criticism by drawing on "institutional endorsements" of the practice (Sanders and Tuschke, 2007). These can include endorsements from

professional CI societies, and associations based on former employment relationships with the national intelligence community[x] which, in professionals` media, are widely accepted as "forces for good" (Kahaner, 1996) (see e.g., IBM in Tables 2.1-2.4). Endorsements allow CI practitioners to distance legitimate "knowledge seeking" from transgressive activities such as espionage. Firms may adapt their CI practices in response to public exposure by replacing executives (e.g., IBM in Table 2.1; 2.3), developing firm-specific ethical codes, (re) training CI professionals (e.g., Unilever, Table 2.4), and outsourcing CI to specialised contractors (e.g., Motorola, Table 2.2). All CI experts across firms emphasised the need for law abidance and noted that considerable investments were needed to ensure compliance with competition laws. Finally, firms adapt organisational structures and the nomenclature used for CI practices, such as "FUD" (fear, uncertainty and doubt) (Manager 12, Oracle). Such adaptation includes reassigning CI professionals to organisational subunits dedicated to benchmarking, knowledge management, data analytics, or more recently, Big Data. This allows firms to deflect criticism by showing that CI is no longer conducted in clandestine or intrusive ways. Adaptation over time thus contributes to practice persistence.

Interdependence among the Factors of Persistence

In conjunction, the factors we identified can allow a stigmatised practice to persist. While keeping the practice opaque protects it from probing scrutiny, it may also sustain a web of beliefs about its indispensability. Moreover, opaqueness may allow the practice to endure

without overt justification or clear evidence of benefits. Contrary to "observability" being a driver of diffusion (Rogers, 1995), "concealability" may be pivotal in the diffusion of stigmatised practices. By keeping CI hidden, practitioners mitigate both the reputational risks from engaging in CI, and the risk of appearing weak and vulnerable as CI victims. CI's "club" shares a sense of privilege (Herman, 1996) and members often agree to out-of-court settlements with competitors rather than expose an industry secret.

> "It seems to be a very small networked cadre of people doing this kind of work. And they all know each other and move around from one company to another. Almost like revolving doors, one builds up quite a network (Manager 8, JLL)

Even fierce rivals agree on the need to avoid public scrutiny (see out-of-court settlements in Tables 3.1-3.2). Yet, efforts to conceal CI are punctuated by scandals. Once dubious practices are exposed, swift changes follow, which includes redefining CI in acceptable terms, and dissociating clean versions from dubious versions of exposed perpetrators (Table 2.3). However, impression management largely represents reactions to favourably influence perception especially during and after scandals. The uneasy equilibrium is disrupted only when scandals temporarily lift the veil. This occurred for example when:

> "This happened at 2 o'clock in the morning and there weren't a lot of people around. Some of the technicians saw some guy taking down notes while looking at the screen of a machine. They didn't know who it was …It turned out he was from a different vendor. So he was gathering information from his competitor. So they chased him out and they found him and his note book … He had taken as much data as he could from the screen. ... So, that was one of our vendors stealing from one of our other vendors."" (Manager 7, Intel)

Keeping CI outside the spotlight avoids close scrutiny of CI's link with performance. Also, setbacks can be attributed to external factors. Dismissing wrongdoers (e.g., scapegoating), (re)

training, (re)enforcements of ethical codes and changing the nomenclature allows a practice to be distanced from a tainted past and allows it to endure by taking on new forms.

CONTRIBUTIONS AND IMPLICATIONS

We explain how and why a stigmatised practice diffuses and persists despite the risks it poses for adopters and how firms are able to dilute the potential stigma from its ongoing use. CI clearly includes legal information gathering but its association with the "grubby" world of spying has arguably tainted the entire CI category. We extend the limited number of studies on practice persistence (Colyvas and Jonsson, 2011; Crane, 2013; Zhu and Westphal, 2011) and on stigmatised practices (Baum and McGahan, 2013; Briscoe and Murphy, 2012; Desai, 2011; Helms and Patterson, 2014) and controversial industries (Humphreys, 2010; Reast et al., 2013; Vergne, 2012). We show how stigmatised practices persist despite risks and the absence of visible performance benefits. While CI can generate commercial gains, engaging in even legal forms of the practice pose reputational risks due to CI's association with illegal use and espionage. Yet, organisations may habitually engage in a practice as an end in itself despite being aware of the risks (Herman, 1996). By refraining from CI, the powerful would be "bad emperors", as "responsible [emperors] were constantly relying on their networks of...spies to find out who was doing his job and who was not" (Fukuyama, 2012: 314). Actors may persist with a practice, not just because of perceived benefits, but because of overestimation of the extent to which others hold this assumption. This is described by Zhu and Westphal (2011) as

"pluralistic ignorance". We show the importance of constructing an "endoxa" – a web of collective beliefs around the utility of a risky practice to justify ongoing use.

The core value proposition of CI is hard to resist; more information is linked to a competitive advantage. The need for more information is in line with the focus on evidence-based decision making (Rousseau, Manning and Denyer, 2008), and the Big Data movement, which offer attractive opportunities for leaving behind the old tainted skin of competitive intelligence. Treating Big Data as if lying on the same trajectory of important innovations may retrospectively legitimise CI and allow it to assume yet another new and equally opaque identity – that of even more encompassing capture and use of data.

Our study has several implications for both theory and practice.

Implications

First, building opaqueness around a stigmatised practice contributes to promoting diffusion (Briscoe and Murphy, 2012). Making a stigmatised practice opaque allows users to engage in the practice without having to demonstrate its benefits. It may thus shield organisations from the scrutiny of audiences and demands for accountability. Thus, while opaqueness is typically thought to impede practice diffusion (Rogers, 1995), it can promote the diffusion in the case of a stigmatised practice.

By studying the diffusion and persistence of CI, we shed light on practices that thrive on opaqueness. The "burden of secrecy" while working with "top-secret" information (Wilensky,

1967: 180), makes it difficult to gauge the effectiveness of intelligence as illustrated in estimating Cuban resistance (Schlesinger, 1965). Besides occasional scepticism and notes of caution that "all that data can be a bother, an unwise expense" and that "large volumes of data present security and reputation risks" (Fitzgerald, 2013), the lack of pressure to prove CI's worth also discourages open debates on its benefits. The diffusion of CI increasingly serves as justification to invest in even more CI (Fleisher, 2008). "Over the years, as CI proliferates to businesses of varying types and sizes, organisations will have to deal with counter intelligence, which is defending company secrets…organisations have to increase and deploy appropriate corporate security to safeguard their data from intelligence efforts by other firms." (Bose, 2008: 524) While CI's hidden costs are now being subsumed under the costs of promoting advanced CI technology, future research can examine the use of mythologised practices that consume valuable resources despite unproven benefits (e.g., Steele, 1975) even when throwing "good money after bad" (Garland, 1990) may not create value for an organisation.

While CI cannot be directly compared with less controversial practices such as consulting and advertising, some of our arguments raise questions about these practices. For example, the benefits of relying on consultants to solve organisational issues remains inconclusive (e.g., De Burgundy; 1998; Wright, 2009), casting doubts on their added value (Gross and Poor, 2008; Sturdy, 2011). Similarly, evidence of the benefits of advertising remains mixed, as

reflected in the truism by John Wanamaker. “Half the money I spend on advertising is wasted. The trouble is I don’t know which half” (Sethuraman, Tellis and Briesch, 2011). It is worth examining how and why these practices continue to persist despite unproven benefits. It is also worth studying how sponsors of lucrative yet risky practices such as arms trading avoid getting scrutinised.

Second, constructing usefulness may justify ongoing use in the absence of transparency and robust measures of performance benefits. Constructing usefulness is often necessary for creating legitimacy around novel practices. An example is buying and selling life insurance policies that had a stigma from putting a “price” to human life. However, it became legitimate once it was associated with concern for family wellbeing (Zelizer, 1978). Similarly trade in human organs that is seen to undermine human dignity is justified for saving lives (Anteby, 2010). However, in the case of stigmatised practices, constructing usefulness is not simply about reframing the practice to justify use and promote adoption. Rather, usefulness is constructed to justify ongoing engagement even in the absence of clearly demonstrable benefits. For example, firms involved in paying commissions (sometimes associated with bribery) and unable to show benefits of such practices may construct usefulness by claiming defensive or unavoidable use in particular contexts.

Third, adapting a practice to enable multiple interpretations (Benders and van Veen, 2001) can promote diffusion. Firms may purposefully create interpretive ambiguity around a

practice to promote a diversity of interpretations (Ansari, Reinecke and Spaan, 2014). Adopters may deny or conceal information that associates the organisation with illegal versions of the practice while continuing with business as usual (Elsbach, 1994; Lamin and Zaheer, 2012), distant themselves from offending versions of the practice (Helms and Patterson, 2014), diversify into non-stigmatised industries (Hudson, 2008), or span multiple categories to divert attention from their association with a stigmatized category (Vergne, 2012). Generating greater interpretive flexibility around a stigmatized practice may thus allow organisations to persist with the practice.

While one of the few studies to examine the development of CI within and across firms, our sample was dominated by large US firms. Our findings may thus have limited transferability for small and medium-sized firms as well as non-US firms. However, as large firms attract the most media attention, it allowed us to capture CI information from public sources and CI experts connected to these firms. Future studies can examine the factors we identified to explain the persistence of other practices and even ideologies, such as shareholder value orientation in different national, industrial and organisational contexts.

REFERENCES

Academic References

Abrahamson, E. (1991). 'Managerial fads and fashions: The diffusion and rejection of innovations', *Academy of Management Review*, **16**, pp. 586-612.

Ahlstrom, D., D. Lamond and Z. Ding (2009). 'Reexamining some management lessons from military history', *Asia Pacific Journal of Management*, **26**, pp. 617-642.

Ahmadjian, C.L., and P. Robinson (2001). 'Safety in numbers: Downsizing and the deinstitutionalization of permanent employment in Japan', *Administrative Science Quarterly*, **46**, pp. 622–654.

Ansari, S., P.C. Fiss and E. Zajac (2010). 'Made to Fit: How practices vary as they diffuse', *Academy of Management Review*, **35**, pp. 67-92.

Ansari, S. Reinecke, J. and Spaan, A. 2014. How are practices made to vary? Managing practice adaptation in a multinational corporation. *Organization Studies.* **35 (9)**: 1313-41.

Anteby, M. 2010. Markets, Morals, and Practices of Trade: Jurisdictional Disputes in the U.S. Commerce in Cadavers. *Administrative Science Quarterly*, 55(4): 606–638.

Armstrong, G., P. Kotler, M. Harker and R. Brennan (2009). *Marketing: An Introduction*. Harlow: Pearson Education.

Baum, J.A.C. and A. McGahan (2013). 'The reorganization of legitimate violence: The contested terrain of the private military and security industry during the post-cold war era', *Research in Organizational Behavior* 33: 3–37

Benders, J. and K. van Veen (2001). 'What's in a fashion? Interpretative viability and management fashions', *Organization*, **8**, pp. 33–53.

Bidwell, M. (2011). 'Paying More to Get Less: The Effects of External Hiring versus Internal Mobility', *Administrative Science Quarterly,* **56**, pp. 369-407.

Bose, R. 2008. Competitive intelligence process and tools for intelligence analysis, *Industrial Management & Data Systems*, 108, 4: 510-528.

Briscoe, F. and C. Murphy (2012). 'Sleight of Hand? Practice Opacity, Third-party Responses, and the Interorganizational Diffusion of Controversial Practices', *Administrative Science Quarterly*, **57**, pp. 553-584.

Calof, J.L. and S. Wright (2008). 'Competitive Intelligence: A practitioners, academic and inter-disciplinary perspective', *European Journal of Marketing*, **42**, pp. 717-730.

Carberry, E.J. and B.G. King (2012). Defensive Practice Adoption in the Face of Organizational Stigma: Impression Management and the Diffusion of Stock Option Expensing, *Journal of Management Studies,* **49:7**, pp.1138-1166.

Carey, T.A. (1999). 'The War Room Guide to Competitive Intelligence', Book Review, *Academy of Management Perspectives*, **13**, pp. 112-113.

Choo, C. W. (1998). *Information management for the intelligent organisation: The art of scanning the environment.* 2nd ed. Medford, NJ: Information Today.
Colyvas, J. and S. Jonsson (2011). 'Ubiquity and Legitimacy: Disentangling Diffusion and Institutionalization', *Sociological Theory*, **29**, pp. 27–53.
Competitive Intelligence Foundation (2006). *State of the Art*. Alexandria, VA: Competitive Intelligence Foundation.
Costas, J. and C. Grey (2014). Organizational Secrecy Bringing Secrecy into the Open: Towards a Theorization of the Social Processes of Organizational Secrecy, *Organization Studies*, DOI: 10.1177/0170840613515470. Published online 24 March 2014
Crane, A. (2005). 'In the company of spies: When competitive intelligence gathering becomes industrial espionage', *Business Horizons*, **48**, 233-240.
Crane, A. (2013). 'Modern slavery as a management practice: Exploring the conditions and capabilities for human exploitation', *Academy of Management Review*, 38, pp. 49–69.
Curtis, J. (2001). 'Behind enemy lines', *Marketing*, May 24, pp. 28-29.
Davis G.F. and H.R. Greve (1997). 'Corporate elite networks and governance changes in the 1980s', *American Journal of Sociology,* **103**, pp. 1–37.
Davison, L. (2001). 'Measuring Competitive Intelligence Effectiveness: Insights from the Advertising Industry', *Competitive Intelligence Review*, **12**, pp. 25-38.
De Burgundy, J. (1998). 'Management consultancy: a modern folly?' *Management Decision*, **36**, pp. 204-205.
Desai, V. M. (2011). 'Mass media and massive failures: determining organizational efforts to defend field legitimacy following crises'. *Academy of Management Journal*, **54**, 263–79.
Dufresne, R. and E. Offstein (2008). 'On the Virtues of Secrecy in Organizations', *Journal of Management Inquiry*, **17**, pp. 102-106.
Eisenhardt, K.M. (1989). 'Building Theories from Case Study Research', *Academy of Management Review*, **14**, pp. 532-550.
Eisenhardt, K.M. and M. E. Graebner (2007). 'Theory building from cases: opportunities and challenges', *Academy of Management Journal*, **50**, pp. 25–32.
Elsbach, K. D. (1994). 'Managing organizational legitimacy in the California cattle industry: The construction and effectiveness of verbal accounts', *Administrative Science Quarterly,* **39**(1): 57-88.
Elsbach, K.D. and R.I. Sutton (1992). 'Acquiring Organizational Legitimacy through Illegitimate Actions: A Marriage of Institutional and Impression Management Theories', *Academy of Management Journal*, **35**, pp. 699-738.
Elsbach, K. D. (2006). *Organizational Perception Management*. Mahwah, NJ: Lawrence Erlbaum Associates.
Fair, W.R. (1966) The corporate CIA – a prediction of things to come, *Management Science*, 12, 10: B489-B503.

Fiss, P., M. Kennedy and G.F. Davis (2012). 'How Golden Parachutes Unfolded: Diffusion and Variation of a Controversial Practice', *Organization Science*, **23**, pp. 1077-1099.
Fleisher, C.S. (2008). 'Using open source data in developing competitive and marketing intelligence', *European Journal of Marketing*, **42**, 7/8: 852-866.
Fitzgerald, M. (2013). 'Turning Big Data Into Smart Data', *MIT Sloan Management Review,* December 02, http://sloanreview.mit.edu/article/turning-big-data-into-smart-data/
Fukuyama, F. (2012). *The Origins of Political Order*. London: Profile Books.
Fuld, L. M. (1995). *The new competitor intelligence: The complete resource for finding, analyzing, and using information about your competitors*. New York: Wiley.
Fuld, L.M. and D.L. Borska (1995). 'What Utilities should expect from competitive intelligence', *Public Utilities Fortnightly*, March 1, pp. 21-24.
Galvin, R.W. (1997). 'Competitive Intelligence at Motorola', *Competitive Intelligence Review*, **8**, pp. 3-6.
Garland, H. (1990). 'Throwing Good Money After Bad: The Effect of Sunk Costs on the Decision to Escalate Commitment to an Ongoing Project', *Journal of Applied Psychology*, **75**, pp. 728-731.
Ghoshal, S. and D. Westney (1991). 'Organizing competitor analysis systems', *Strategic Management Journal*, **12**, pp. 1-15.
Gilad, B. (1996). *Business Blindspots – Replacing Your Company's Entrenched and Outdated Myths, Beliefs and Assumptions With the Realities of Today's Markets,* Chicago, IL: Probus Publishing Company.
Gioia, D.A., K.N. Price, A.L. Hamilton and J.B. Thomas (2010). 'Forging an Identity: An Insider-outsider Study of Processes Involved in the Formation of Organizational Identity', *Administrative Science Quarterly*, **55**, pp. 1-46.
Glick, W. H., G. R Huber, C. C. Miller, D. H. Doty, and K. M. Sutcliffe (1990). 'Studying changes in organizational design and effectiveness: Retrospective event histories and periodic assessments', *Organization Science*, **1**:293-312.
Godfrey, R., J. Brewis, J. Grady and C. Grocott (2012). 'The private military industry and neoliberal imperialism: Mapping the terrain', *Organization*, published online, doi: 10.1177/1350508412470731
Green, S. E., Y. Li and N. Nohria (2009). 'Suspended in Self-Spun Webs of Significance: A rhetorical model of institutionalization and institutionally embedded agency', *Academy of Management Journal*, **52**, pp. 11-36.
Greve, H. R. (1995). 'Jumping Ship: The Diffusion of Strategy Abandonment', *Administrative Science Quarterly*, **40,** pp. 444-473.
Greve, H., D. Palmer and J-E. Pozner (2010). 'Organizations Gone Wild: The Causes, Processes, and Consequences of Organizational Misconduct', *The Academy of Management Annals,* **4**, pp. 53–107.

Grey, C. (2009). 'Security Studies and Organization Studies: Parallels and Possibilities', *Organization*, **16**, pp. 303-316.
Gross, A. and J. Poor (2008). 'The Global Management Consulting Sector', *Business Economics*, October, **43**, pp. 59-68.
Hannula, M. and V. Pirttimaki (2003). 'Business Intelligence: Empirical Study on the top 50 Finnish Companies', *Journal of American Academy of Business*, **2**, pp. 593-599.
Helms, W. and Patterson, K. (2014). 'Eliciting Acceptance for 'Illicit' Organizations: The Positive Implications of Stigma for MMA Organizations', *Academy of Management Journal*, 57:1453-1484.
Hemphill, T. A. (2002). 'Oracle vs. Microsoft: Corporate Espionage or Competitive Intelligence?' *Business and Society Review*, **107**, pp. 501-511.
Herman, M. (1996). *Intelligence Power in Peace and War*, Cambridge: Cambridge University Press.
Herring, J. (1996). *Measuring the Value of Competitive Intelligence: Accessing & Communicating CI's Value to Your Organization*, SCIP Monograph Series, Alexandria: SCIP.
Herring, J. (1999). 'Key Intelligence Topics: A Process to Identify and Define Intelligence Needs', *Competitive Intelligence Review*, **10**, pp. 4-14.
Hirsch, P. M. and D. Z. Levin, (1999). 'Umbrella advocates versus validity police: A life-cycle model', *Organization Science*, **10**, pp. 199-212.
Houston, P., M. Floyd, S. Carnicero, D. Tennant (2012). *Spy the Lie: Former CIA Officers Teach You How to Detect Deception*, New York: St. Martin`s Press
Howard, M. (2011). 'The Transformation of Strategy', *The RUSI Journal*, **156**, pp. 12-16.
Huber, G. P, and D. J. Power (1985). 'Retrospective reports of strategic-level managers: Guidelines for increasing their accuracy', *Strategic Management Journal*, 6: 171-180.
Hudson, B. A. (2008). Against all odds: A consideration of core-stigmatized organizations. *Academy of Management Review*, 33: 252–266.
Humphreys, A. (2010). 'Megamarketing: The Creation of Markets as a Social Process', *Journal of Marketing*, 74 (2): 1-19.
Jack, L. (2005). 'Stocks of Knowledge, simplification and unintended consequence: The persistence of post-war accounting practices in UK agriculture', *Management Accounting Research*, **16**, pp. 59-79.
Jameson, D. A. (2011). 'The Rhetoric of Industrial Espionage: The Case of Starwood V. Hilton', *Business Communication Quarterly*, **74**, pp. 289-297.
Jaworski, B.J., D.J. Macinnis and A.K. Kohli (2002). 'Generating Competitive Intelligence in Organizations', *Journal of Market-Focused Management*, **5**, pp. 279-307.
Jick, T. D. (1979). 'Mixing qualitative and quantitative methods: Triangulation in action', *Administrative Science Quarterly*, **24**: pp. 602-611.
Jones, G. (2002). 'Control, performance, and knowledge transfers in large multinationals: Unilever in the United States, 1945-1980', *Business History Review*, **76**, pp. 435-478.

Jones, C. (2008). 'Editor's Introduction' [to a special section on Secrecy], *Journal of Management Inquiry*, **17**, pp. 95-96.
Jonsson, S. and H. Buhr (2011). 'The Limits of Media Effects: Field Positions and Cultural Change in a Mutual Fund Market', *Organization Science*, **22(2)**, pp. 464-481.
Jonsson, S., H. Greve and T. Fujiwara-Greve (2009). 'Undeserved Loss: The Spread of Legitimacy Loss to Innocent Organisations in Response to Reported Corporate Deviance', *Administrative Science Quarterly*, **54**, pp. 195-228.
Kahaner, L. (1996). *Competitive Intelligence: From Black Ops to Boardrooms – How Businesses Gather, Analyze, and Use Information to Succeed in the Global Marketplace*, New York: Simon & Schuster.
Kara, S. (2009). *Sex trafficking: Inside the business of modern slavery.* New York: Columbia University Press.
Kennedy, M. and P. Fiss. (2009). 'Institutionalization, Framing, and Diffusion: The Logic of TQM Adoption and Implementation Decisions among U.S. Hospitals', *Academy of Management Journal, **52**,* pp. 897-918.
Kets de Vries, M. (1989). 'Can you survive an entrepreneur?' In J. Kao (Ed.) *Entrepreneurship, Creativity and Organisation*, pp. 157-165. Englewood Cliffs, N.J.: Prentice-Hall,
Kieser, A. (1997). 'Myth and rhetoric in management fashion', *Organization*, **4**, pp. 49-74.
Lamin, A. and S. Zaheer (2012). 'Wall Street vs. Main Street: Firm strategies for defending legitimacy and their impact on different stakeholders', *Organization Science*, **23(1)**: 47-66.
Lounsbury, M. (2007). 'A Tale of Two Cities: Competing Logics and Practice Variation in the Professionalizing of Mutual Funds', *Academy of Management Journal*, **50**, pp. 289–307.
Martin, K., J. Cullen, J., Johnson and P. Parboteeah (2007). 'Deciding to bribe: A cross-level analysis of firm and home country influences on bribery activity', *Academy of Management Journal,* **50**, pp. 1401–1422.
McKenna, S.D. (1996) 'The darker side of the entrepreneur', *Leadership & Organisation Development Journal*, **17**, pp. 41-45.
Meyer, J. and B. Rowan (1977). 'Institutionalized Organisations: Formal Structure as Myth and Ceremony', *American Journal of Sociology,* **83**, pp. 340-363.
Nasheri, H. (2005). *Economic Espionage and Industrial Spying*. Cambridge University Press.
Nolan, J. (1999). *Confidential: Uncover Your Competitors' Top Business Secrets Legally and Quickly – and Protect Your Own*. New York: Harper Business.
Ocasio, W. and J. Joseph (2008). 'Rise and Fall or Transformation: The Evolution of Strategic Planning at the General Electric Company, 1940-2006', *Long Range Planning*, **41**, pp. 248-272.
Pepper, J.E. (1999). 'Competitive Intelligence at Procter and Gamble', *Competitive Intelligence Review*, **10**, pp. 4-9.
Pfaff, D. (2005). *Competitive Intelligence in der Praxis*. Campus: Frankfurt am Main.

Price, K.N., D.A. Gioia, K.G. Corley (2008). 'Reconciling Scattered Images: Managing Disparate Organizational Expressions and Impressions', *Journal of Management Inquiry*, **17**, pp. 173-185.

Reast, J., Maon, F., Lindgreen, A. and Vanhamme, J. (2013). 'Legitimacy-Seeking Organizational Strategies in Controversial Industries: A Case Study Analysis and a Bidimensional Model', *Journal of Business Ethics*, 118: 139-153.

Richardson, L. and V. Luchsinger (2007). 'Strategic Marketing Implications in Competitive Intelligence and the Economic Espionage Act of 1996', *Journal of Global Business Issues,* summer, **1**, pp. 41-45.

Rogers, E. M. (1995). *The diffusion of innovations* (4th ed.). New York: The Free Press.

Rousseau D, Manning J, Denyer D (2008). 'Evidence in management and organizational science: Assembling the field's full weight of scientific knowledge through syntheses', *Academy of Management Annals*, 2, 475-515.

Saayman, A., J. Pienaar, P.J. de Pelsmacker, W. Viviers, L. Cuyvers, M-L. Muller and M. Jegers (2008), 'Competitive Intelligence: Construct Exploration, Validation and Equivalence', *Aslib Proceedings: New Information Perspectives*, **60**, pp. 383-411.

Sanders, W.G. and A. Tuschke (2007). 'The adoption of institutionally contested organisational practices: The emergence of stock option pay in Germany', *Academy of Management Journal,* **50**, pp. 33–56.

Schelling, T. C. (2007). *Strategies of commitment and other essays*. Cambridge, MA: Harvard University Press.

Schlesinger, A.M. (1965). *A Thousand Days: John F. Kennedy in the White House*, Boston: Houghton Mifflin.

Sethuraman, R., G. Tellis and R. Briesch (2011). 'How well does Advertising Work? Generalizations from Meta-Analysis of Brand Advertising Elasticities', *Journal of Marketing Research*, **48**, pp. 457-471.

Soin, K. and C. Huber (2012). 'The Sedimentation of an Institution: Changing Governance in U.K. Financial Services', *Journal of Management Inquiry*, first published on December 26, 2012 as doi:10.1177/1056492612467510.

Steele, F. (1975). *Consulting for organizational change*. Amherst: University of Massachusetts Press.

Sturdy, A. (2011). 'Consultancy's Consequences? A Critical Assessment of Management Consultancy's Impact on Management', *British Journal of Management*, **22**, pp. 517-530.

Swartz, N. (2005). 'Competitive intelligence underutilized', *Information Management Journal*, **39**, p. 10.

Taussig, M. (1999). *Defacement: Public Secrecy and the Labor of the Negative*. Stanford, CA: Stanford University Press.

Tellis, G. (2009), 'Generalizations About Advertising Effectiveness in Markets', *Journal of Advertising Research*, **49**, pp. 240-245.

Terlaak, A. and Y. Gong (2008) 'Vicarious Learning and Inferential Accuracy in Adoption Processes', *Academy of Management Review*, **33**, pp. 846-868.
Todd, P. and J. Bloch (2003). *Global Intelligence: The World`s Secret Services Today*. London and New York: Zed Books.
Tolbert, P. S. and L. G. Zucker (1983). 'Institutional Sources of Change in the Formal Structure of Organisations: The Diffusion of Civil Service Reform, 1880-1935', *Administrative Science Quarterly*, **28**, pp. 22-39.
Vaccaro, A. and Palazzo, G. 2014. 'Values against Violence: Institutional Change in Societies Dominated by Organized Crime', Forthcoming in *Academy of Management Journal.*
Vergne, J. P. 2012. 'Stigmatized categories and public disapproval of organizations: A mixed-methods study of the global arms industry, 1996–2007'. *Academy of Management Journal*, 55: 1027–1052.
Verhoef, P. C. and P. S. H. Leeflang (2009). 'Understanding the Marketing Department`s Influence Within the Firm', *Journal of Marketing*, **73**, pp. 14-37.
Wallensteen, P. and M. Sollenberg (1996). 'The End of International War? Armed Conflict between 1989-95', *Journal of Peace Research*, **33**, pp. 353-370.
Westphal, J. D., Gulati, R. and S.M. Shortell (1997). 'Customization or conformity? An institutional and network perspective on the content and consequences of TQM adoption', *Administrative Science Quarterly*, **42**, pp. 366-394.
Whitney, M.E. and J. D. Gaisford (1999). 'Why Spy? An Inquiry into the Rationale for Economic Espionage', *International Economic Journal*, **13**, pp. 103-123.
Wilensky, H. (1967). *Organisational Intelligence: Knowledge and Policy in Government and Industry.* New York: Basic Books
Wright, C. (2009). 'Inside out? Organisational membership, ambiguity and the ambivalent identity of the internal consultant', *British Journal of Management*, **20**, pp. 309–322.
Wright, P. C. and G. Roy (1999). 'Industrial espionage and competitive intelligence: one you do; one you do not', *Journal of Workplace Learning*, **11**, 2, pp. 53-59.
Zelizer, V. A. (1978). 'Human Values and the Market: The Case of Life Insurance and Death in 19th-Century America', *American Journal of Sociology*, **84** (3) pp. 591–610.
Zhu, D. and Westphal, J. (2011). 'Misperceiving the beliefs of others: How pluralistic ignorance contributes to the persistence of positive security analyst reactions to the adoption of stock repurchase Plans', *Organization Science*, Vol. **22**, No. 4, pp. 869–886.

Empirical References

ACI (2014) – Academy of Competitive Intelligence, accessed on line; January 2014; http://www.academyci.com/
Arensman, R. (2001). 'Shedding the trench coat', *EDN*, September 1, from

http://www.edn.com/article/print/490112-Shedding_the_trench_coat.php
Armitstead, L. (2012). 'Dyson sues after discovering German "spy" on its staff', *Telegraph*, Wednesday, October 24.
Clark, N. (2013). 'Revelations that Ikea spied on its employees stir outrage in France', *The New York Times*, December 15; accessed on line.
Cohen, N. (2013). 'Surveillance: Cozy or Chilling?' *The New York Times*, December 14; accessed online.
Dodd, C. (2013). 'Technology isn't to blame for espionage', Turbine, accessed on line, http://turbinehq.com/2013/technology-not-to-blame-for-espionage/
Green, W. (1998). 'I SPY: Your competitor is snooping on you. So what's wrong with that?' *Forbes*, **161**, April 20, pp. 90-100.
Heavens, A. and M. Leising (2001). 'Companies walk ethical tightrope: *Competitive Intelligence*', *Financial Times*, April 10, p. 4.
Holmes, A. (2013). 'NSA Spying Seen Risking Billions in U.S. Technology Sales', *Bloomberg*, September 10, 2013, http://www.bloomberg.com/news/print/2013-09-10/nsa-spying-seen-risking-billions-in-u-s-technology-sales.html
Houston, P., M. Floyd, S. Carnicero, D. Tennant (2012). *Spy the Lie: Former CIA Officers Teach You How to Detect Deception*, New York: St. Martin`s Press
Javers, E. (2010). *Broker, Trader, Lawyer, Spy: The Secret World of Corporate Espionage*, New York: Harper Business.
King, N. and J. Bravin (2000a) 'Call It Mission Impossible Inc. – Corporate Spying Firms Thrive', *Wall Street Journal*, July 30, B1.
King, N. and J. Bravin (2000b) 'Corporate-Spying Firms Thrive: CIA Veterans, Dumpster-Divers Work in "Competitive Intelligence": If the Trash is on the Curb, It`s Fair Game', *Wall Street Journal*, July 4, Europe Edition.
Lauria, J. (2000). 'Oracle caper lifts lid on America's Corporate Spies', *The Sunday Times*, July 9, accessed online.
Moffett, S. and D. Pearson (2011). 'Ghosn: Cost Data Key to Renault Spy Case', *Wall Street Journal*, February 11, accessed online,
http://online.wsj.com/article/SB10001424052748703310104576134803371815280.html
Nelson, E. and S. Ellison (2001). 'Unilever and P&G Reach Settlement in Espionage', *Wall Street Journal*, September 7, B6.
Nolan, J. (1999). *Confidential: Uncover Your Competitors' Top Business Secrets Legally and Quickly – and Protect Your Own*. New York: Harper Business.
O'Reilly, T. and J. Battelle (2009) '*Web Squared: Web 2.0 Five Years On*', Special Report, accessed online, http://assets.en.oreilly.com/1/event/28/web2009_websquared-whitepaper.pdf
Penenberg, A., and M. Barry (2000). *Spooked: Espionage in Corporate America*, New York: Perseus.
Pikas, C. K. (2005). 'Blog Searching for Competitive Intelligence, Brand Image, and

Reputation Management', www.onlinemag.net, July/Aug, page 16-21.
Rogers, M. and D. Ruppersberger (2012). *Investigative Report on the U.S. National Security Posed by Chinese Telecommunications Companies Huawei and ZTE*, Permanent Select Committee on Intelligence, U.S. House of Representatives, 112th Congress, October 8, accessed online, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf
Salmon, R. and Y. de Linares (1999). *Competitive Intelligence: Scanning the Global Business Environment*, London: Economica.
Schimroszik, N. (2012). Dyson accuses Bosch of paying research spy, *The Guardian*, October 24, accessed online. http://www.guardian.co.uk/business/2012/oct/24/dyson-accuses-bosch-paying-research-spy.
SCIP (2013). Society of Competitive Intelligence Professionals, www.scip.org
Sorensen, C. (2004). 'Cloak & Dagger Inc.', *National Post*, July 8, FP1 Front.
Stone, B. (2000). 'Diving into Bill's trash', *Newsweek*, **136**, p. 49
Teitelbaum, R. (1992). 'The New Race for Intelligence: Your Competitors May Well be Mounting Sophisticated Information-Gathering Operations,' *Fortune,* **126**, pp. 104-107.
The Economist, (2011). 'The Renault "spying" affair: A new twist', *The Economist*, March 10, accessed online, http://www.economist.com/node/18332938
The Economist (2013a). 'The bloodhounds of capitalism: It is a good time to be a corporate investigator', *The Economist*, January 5, accessed online, http://www.economist.com/news/business/21569028-it-good-time-be-corporate-investigator-bloodhounds-capitalism
The Economist (2013b). 'We snoop to conquer: Security cameras are watching honest shoppers, too', *The Economist*, February 9, accessed online, http://www.economist.com/news/business/21571452-security-cameras-are-watching-honest-shoppers-too-we-snoop-conquer.
Todd, P. and J. Bloch (2003). *Global Intelligence: The World`s Secret Services Today*. London and New York: Zed Books.
Wilson, L. (2001). 'Tech 'spies' work overtime at Sun, Oracle, Microsoft', *San Francisco Business Times*, February 4 (Sunday), http://www.bizjournals.com/sanfrancisco/stories/2001/02/05/story3.html?t=printable
Wong, W. (2000). 'Oracle Chief defends Microsoft Snooping', *CNET News.com*, June 28, accessed online, http://technews.netscape.com/news /0-1003-200-2167548.html.
Worth, R.F. (2013). 'The Spy Novelist Who Knows Too Much', *The New York Times*, January 30, accessed online, http://www.nytimes.com/2013/02/03/magazine/gerard-de-villiers-the-spy-novelist-who-knows-too-much.html?pagewanted=all&_r=0

Appendix 1: Definition of CI

Investigating rivals and industrial espionage is clearly *not* the same thing. Spying is often illegal and always unethical; CI gathering is legitimate (Fleisher, 2008; Bose, 2008: 510). The 1996 Economic Espionage Act clearly made stealing or appropriating proprietary information illegal with fines up to $10 million and penalties up to 15 years in prison. CI has grown dramatically as more and more companies conduct CI on their competitors (Rogers and Ruppersberger, 2012). While such gathering and analysing strategic information is seen to be a legitimate practice, and all CI professional activities to gather digital and non-digital information are subsumed under CI (SCIP, 2013; Bose 2008), the way information is gathered and treated can arouse suspicion.

However, the media show how legal CI activities can be confounded with rogue acts that may taint CI users (Dodd, 2013). Here, corporate detectives "sniff out the facts", and companies are increasingly hiring corporate-intelligence firms to investigate their rivals (The Economist, 2013a), clients (Holmes, 2013), employees (Clark, 2013), and even consumers (The Economist, 2013b). For outsiders and in the media, the boundary between legally gathering intelligence on rivals and illegally spying on them through traditional or digital means is blurry (Green, 1998; Curtis, 2001; Cohen, 2013; Pikas, 2005; Teitelbaum, 1992) and illegal practice remains. "[I]n 1997, there were more than 1,100 documented cases of economic espionages related to intellectual property worth over $300 billion" (Carey, 1999: 112). This can lead to clients and others suspecting even legitimate CI (Holmes, 2013).

In the media, some CI professionals reveal that part of the job is "tracking down the disgruntled former secretary or bookkeeper who knows where the bodies are buried and knowing how to coax information from them" (The Economist, 2013: 7a). "It's as close as I'll get to playing James Bond without being shot at," said the president of a firm conducting CI for companies (Parker, 2002: 1). "We'll bug a house, bug cars, put locator devices on vehicles, conduct electronic intercepts of e-mails, whatever it takes. …But we won't break the law…wherever we're operating. Otherwise, the information we collect is useless to our clients" because illegally collected evidence is not permitted as evidence in courts and would undermine any lawsuit (Javers, 2010: 227-228).

Yet, "[t]he most useful information tends to be the most carefully guarded, meaning normal channels of corporate intelligence are unlikely to prove fruitful. And if you do it in an ethical fashion, you're simply not going to get the same quality of information as if you do it unethically." (Sorensen, 2004: FP1 Front). A CI consultant noted: "It all comes down to how much they are willing to pay. Basically, any type of information can be discovered, given enough money, but at times that will go into the illegal aspects. In my experience, a lot of people go over the line – they just don't get caught" (Heavens & Leising, 2001: 4).

Therefore, the line between legitimate CI and illegal espionage is clearly not distinct, which makes CI a prominent exemplar of a stigmatised practice.

Appendix 2: Data Sources

Gathering data on CI is not easy. We offer four explanations for how we overcame the challenge of data access. First, since the fall of the Soviet Union and 9/11, "the covert world [has come] under unprecedented public scrutiny" (Todd and Bloch, 2003: I). The release of intelligence sources has led to a surge in economic espionage as military allies turned into vigorous economic competitors (Whitney and Gaisford, 1999). Second, organisations in the modern digital media environment have a "scattered images" problem (Price, Gioia and Corley, 2008: 173) and "information shadows" (O'Reilly and Battelle, 2009; The Economist, 2013b). We reconstructed the scattered data on companies' activities from disconnected but available reports across a variety of media. Third, investigative journalism is flourishing as part of media`s role in exposing deviant firms (Jonsson and Buhr, 2011; Desai, 2011). For example, novelists tap into and disseminate secrets by "cultivating spies and diplomats, who seem to enjoy seeing themselves and their secrets transfigured into pop fiction (with names carefully disguised)" and reveal "terror plots, espionage and wars" ahead of the news or even the events themselves (Worth, 2013). Fourth, the anthropological notion of "public secrets", i.e., "what is generally known but cannot be articulated" (Taussig, 1999: 6) may apply to CI.

We identified relevant industries and companies through archival data. We used key terms (such as competitive intelligence, competitor intelligence and market intelligence) to capture public data on CI practices from databases such as AIB/Inform, Business Source Premier, Factiva, Mergent Online and Lexis-Nexis. We chose the period between 1985 and 2005 in which data availability was relatively high. We gathered about 28,000 documents that contained the words "competitive" and "intelligence" and then eliminated all advertisements. To avoid double counts, we focused on 3,978 articles available on ABI/Informs with CI in the title. In 1985, six media articles mentioned CI in the title (Figure 1). This rose to 40 articles in 1997, 165 in 2000, and 472 in 2005. Since 2005, ABI/Inform shows 3,978 articles with CI in the title, with peaks in 2008 (672) and in 2011 (661). We compared these results with those generated for the same keywords in texts by Google ngrams until 2008, and found them supportive of the chosen period's importance for CI. On this basis, we selected 1985 as the start year and 2012 as the end year. We analysed over 3,000 abstracts and articles based on the words "competitive intelligence" published online, and in journals, books, and the media to gain an overview.

Table 1: Interviewees with Managers and CI Experts in Case Companies

Interviewee Number	Industry	Company CI association	Company Experience	Experience with CI	Other Experience	Experience (years)	Current Position, Function
1	Business Services	Low	**IBM**	Provider and client	Entrepreneur, Retail, Business-to-Business, International Experience	10+	Middle Management, Consulting
2	Business Services	Low	**IBM**	Provider and client	Strategy Consulting, International Experience	30+	Middle Management, Sales
3	Business Services	Low	**IBM**	Client	Multiple business units	20+	Middle Management, Sales
4	Business Services	Low	**IBM**	Client	Multiple business units	20+	Middle Management, Sales
9	Business Services	Low	**Microsoft**	Client	Electronics, International Experience	15+	Middle Management, Sales
11	Business Services	High	**Oracle**	Provider and client	International Experience	15+	Middle Management, Sales
12	Business Services	High	**Oracle**	Provider and client	Research and Consulting, International Experience	20+	Self-employed
6	Electronic Equipment	High	**Intel**	Client	International Experience	15+	Middle Management, Engineering
7	Electronic Equipment	High	**Intel**	Provider and Client	Functional Experience	10+	Entrepreneur
5	Electronic Equipment	-	**IFT**	Client	SME	20+	Managing Director
10	Electronic Equipment	Low	**Motorola**	Provider and client	Business Services, Electronic Equipment, Consumer Hardware	30+	CEO
13	Fast Moving Consumer Goods	Low	**Procter & Gamble**	Client	Fast Moving Consumer Goods, International Experience	5+	Middle Management, Market Research
14	Fast Moving Consumer Goods	Low	**Unilever**	Client	Fast Moving Consumer Goods	20+	Middle Management, New Business Development
8	Real Estate	-	**JLL**	Provider and client	Real Estate, International Experience	10+	Advisor

Table 2.1: Company Cases and CI Development (IBM and Linear Technologies)

Company (CI relatedness (a))	**Antecedent**	**1980s**	**early 1990s**	**late 1990s**	**early 2000s**	**late 2000s**	**early 2010s**
IBM (low)	Victim of foreign "moles" in EU; arrests related to confidential material; emphasised mainframe, missed trend of desktop computing by individual users	CI efforts focus on technology trends aiming for best practice	Top management involvement; 1993: Gerstner sets up a squad of CI teams, led by senior executives as customer experts; growing diversity in cross-functional CI team; diffusion of best practice by hiring former CIA veteran as CI consultant, J. Herring (see TI, Motorola); virtual CI teams	1998: standard CI on rivals` products prior to launch, discount, sales pitches; CI`s "human intelligence network; growing diversification of targets competitors' clients, consultants, suppliers, and rivals` young engineers; seeks patterns in fragmented data (Big Data); technological standardisation with net-based technologies; known as "eagle" (leading CI firm); Herring and Gilad, a CI consultant to IBM and P&G found Academy of CI	2000: Includes CI as a part of corporate strategy; 2001: one of leading three users of CI; rise of standardisation formalisation; 2005: More centralisation; officer responsible for CI per region; formal CI training for employees; CI focus on competitors and prevention of reputational damage; IBM widely known as exemplar if best practice; Herring and Gilad merge training organisation with Fuld	CI becomes mainstream business; acquires firms in business applications space; widely studied as best practice and as major player in CI software	After acquiring Cognos, leading player that benefits from rising importance of specialisation in analytics; key player in package software and licenses for CI (e.g. Big Data); ranked as top US corporate CI user; seen as best practice and CI target, identified as the company with largest number of business lines (626); key player in security industry
Linear Techno-logics (low)		1986: aims for best practice; R&D focused on world patent register; scientific trends to spot opportunities		1996: LT sued by Maxim Integrated Products for theft of trade secrets (posing as customer) ; Damage control: settles dispute out of court; 1998: rise in scale/scope; CI units within R&D analyse end-user trends; adhering to standard CI practice	2000: adhering to standard practice, CI for alerts on trends: e.g. portability, connectivity, processing power; LT changed direction to focus on power usage and battery life; R&D, marketing share intelligence across units (diversity of users and producers)	known as best practice in knowing end users` technology needs	

(a) based on associations with CI in WSJ

Table 2.2: Company Cases and CI Development (Microsoft and Motorola)

Company (CI relatedness)	**Antecedent**	**1980s**	**early 1990s**	**late 1990s**	**early 2000s**	**late 2000s**	**early 2010s**
Microsoft (low)		1987: Top management involved; New marketing VP focuses on gathering customer intelligence	1992: growth in scale and scope; CI units within product units	1997-1999: Top executives involved; CEO dedicates time to CI, creates feedback loop driving priorities, increases scale/scope; spends more on CI related IT/services; increases the diversity of CI users/producers; firm known as "eagle", i.e. leading CI firm; standardisation with net-based technologies	2000: Adopts CI Dashboard standard for executives ; external experts and CI staff actively gather CI; 2001: Named as leading user of CI; 2002: Victim of transgressive dumpster diving; found to support interest groups; damage control by settling dispute out of court; 2004: transgression by employees` under cover activities at competitor`s convention; damage control by policy changes; ranked as one of the most searched companies online; success viewed as cause for turning into target for security breaches and attacks such as hacking, phishing; former leaders of CI leave and start CI focused firms	Invests in CI related software as core; acquires CI related firms in advanced B2B applications space; best practice case in CI books by leading CI authors (Fuld); listed as leading player in CI software; CI products have advantage with familiar interface	Known as top player; exploits rising importance of specialised software for business analytics; a leading player in CI related package software and licenses (Big Data)
Motorola (low)	CEO R. Galvin, member of US President's Foreign Intelligence Advisory Board, 1970s	CEO, top team driving; industry's first formal CI programs; CEO recruits 20 year veteran CIA officer J. Herring in 1982 (see TI, IBM); CI expert in each of five divisions; tech-focussed CI unit; 10 people at corporate level, $1m budget; diverse team (finance, politics, Japanese management); five operational divisions with own CI unit; technology CI for Iridium project		1995: Increasing scale and scope; Broadens focus to include outside change, the whole competitive environment (regulatory, tech, market, industry); needs identification process 1998: IT a multiplier for CI; acknowledged as "eagle" leading CI company; prominent CI leaders Herring and Gilad, a CI consultant also to IBM and P&G found Academy of CI	2000: Develops a professional human-source intelligence collection operation to tap brains of 90,000 employees worldwide (high diversity of users and producers of CI); 2001: Among the leading five users of CI across industries (high degree of formalisation by benchmarking); 2004: Enterprise Roadmap Management System; roadmap library for collaborative sharing; Motorola widely acknowledged as pioneer of CI and best practice; well known for CI capabilities; case study in best practice studies; Robert Galvin acclaimed as driver behind CI; former leaders of CI leave and establish CI focused companies; seen as virtual organisation prone to rely on subcontracting and IT both increasing likelihood of security breaches; Herring and Gilad merge training organisation with other CI consultant, L. Fuld,	Motorola widely acknowledged as pioneer of CI and best practice; former Motorola CI leaders establish CI consultancies	Widely acknowledged pioneer of CI

Table 2.3: Company Cases and CI Development (Procter & Gamble and Unilever)

Company (CI relatedness)	**Antecedent**	**1980s**	**early 1990s**	**late 1990s**	**early 2000s**	**late 2000s**	**early 2010s**
P&G (low)	Increasing speed of change; victim of CI transgression (settled at $125 m)	1988: First global multi-sector analysis; aiming for best practice establishes corporate CI (Hub and Spokes structure); benchmarks in 6 month cycles common CI practice	Benchmarking in 6 month cycles common CI practice; adoption of best practice by hiring of leading professionals; Ex-FBI officer leads security, regular checks of ad agencies, vendors, reporters by video, phone, observation on trips to protect secrets; 1993: CI led by Steinhardt (until 2000)	Top management involved; acknowledged as "eagle", i.e. leading CI company; CEO support for CI; Global Knowledge Network (digital Hub & Spoke); standardisation with net-based technologies; increase of scale and scope; dynamic modelling of competition; Intranet; CI training; CI part of strategic planning process; former CEO (initiator of CI at Motorola) joins board; diffusion of best practices; CI uses safe house and a head office (known as 'the ranch' and 'Kremlin'); limits official contacts outside of firm; prominent CI leaders Herring and Gilad, a consultant to P&G and IBM found Academy of CI	Sourcing of global CI portal; Top management involved; in 2000 Chairman, ex-CEO J. Pepper (1999) states CI should be embedded in the formal strategic process and a standard process at all levels; boost to diversity of users and producers of CI; transgression and reputation damage after P&G revealed that its CI contractors had spied on Unilever's hair-care unit; damage control by immediate departure of three executives directly involved; settles dispute out of court in 2001 for $10 m; P&G one of five top users of CI; formalisation and standardisation increase as former P&G executive becomes CEO of key competitor; company standards forbid employees/ suppliers to work on laptops on planes to avoid leaks; P&G well known for CI capabilities; Herring and Gilad merge training organisation with that of other CI consultant, Fuld	Included in benchmarking studies and acknowledged as best practice	P&G widely acknowledged to be a leading company; utilizing CI and benchmarking (for period 1988-1997); P&G analysed as best practice in benchmarking studies
Unilever (low)	Victim of transgressive CI by competitor's subcontractor; Damage control by settling dispute out of court		CI deploys patent tracking	Widespread CI training to collect and to protect intelligence	Random checks on internal security (actors infiltrate employees` groups and identify leaks); policies forbid employees or employees of suppliers to work on laptops in airplanes to limit espionage risk; CEO of Unilever is former P&G employee and holder of P&G shares and stock options	Included in benchmarking studies and acknowledged as best practice	

Table 2.4: Company Cases and CI Development (Intel, Oracle and Texas Instruments and Unisys)

Company (CI relatedness)	**Antecedent**	**1980s**	**early 1990s**	**late 1990s**	**early 2000s**	**late 2000s**	**early 2010s**
Intel (high)	1980s: Threat of Japanese rivals; 1999: surprised by low-cost PCs; lost share	First moves to establish best practice in response to threat from Japanese rivals	1992: Focus on technology, competitors' progress with specific technologies	1996: Hires ex CIA officers, experts in disinformation; agencies` as model (see IBM, TI, Motorola); primary data; aims at best practice; known "eagle", savviest US CI firm; rising CI scale/ scope; formalized, diverse CI people	Top team involved; A. Grove, CEO integrates KM/CI in "dashboard"; formalized contents; net-based standards ; among most searched firms online; known as best practice, sponsor/ promoter of CI	known as best practice with dedicating staff fully to CI; significant investments	contributes to increasing memory and capacity of large repositories used for Big Data
Oracle (high)		1988: Gathering and analysing intelligence on targeted market segments	1995: Establishes intelligence function aiming for best practice	Reward systems to incentivise internal diffusion of CI through sharing of customer and competitor information across different units (growing diversification of users and producers of CI)	2002: Contractor transgressive (dives dumpster at Microsoft affiliate); executive departure; reputation/ share price hurt; damage control: out of court settlement	Corporate CI; integrates databases; standards, net-based; one of the most searched firms online; invests in CI software as mainstream; acquires CI related firms in advanced software; major player: CI enterprise software	Known as mayor player exploiting rising importance of specialised software for analytics; remains leading player in packages, licenses for Big Data CI software
Texas Instruments (high)	Victim of foreign espionage activities	1987: Technology; R&D	1993: scope grows; aims for best practice; top executives involved; hires CI experts; adopts approach of professionals	CI scale/scope grows; crosses depts.; central CI unit; for all compulsory training; diverse CI producers/ users; Key CI Topics (Herring, 1996; 1999), US Gov. best practice (see IBM, Intel, Motorola); Herring joins Gilad, P&G, IBM advisor, to found Academy of CI; CI prepares M&A	CI efforts acknowledged as effective best practice to avert disadvantage; Herring and Gilad merge training organisation with that of CI consultant Fuld	Acknowledged as best practices in CI by practitioner and academic audience	
Unisys (high)		1988: Decentralise Each group with R&D intelligence staff; increase of scale	1994: CI shifts from technology to customer focus; CI units diffuse to all customer segments to gain industry knowledge; cross section CI sessions; focus on CI standards	1999: Establishes centralised intelligence unit, as staff function; standardisation of approach; input for new leadership team's strategic planning processes	2004: CI for communities with common purpose; diverse CI producers/ users; professional CI capabilities/motivation grown; knowledge, best practice sharing; partners with software provider to offer standardized CI related solutions; strategic alliance with CIA funded intelligence firm	Internal search for CI best practices; award for CI practices to share insights; CI as (part of) customised service and consulting	Global player in security industry

Table 3.1: Cross Case Analysis (IBM, Linear Technology, Microsoft, Motorola, P&G and Unilever)

Company (CI association)	**IBM** (low)	**Linear Technology** (low)	**Microsoft** (low)	**Motorola** (low)	**Procter & Gamble** (low)	**Unilever** (low)
Antecedents	· Victim of espionage · Settled out of court	· CI scandal · Settled out of court	· CI scandal · Settled out of court	· CEO insider of US CI community	· Victim of espionage; CI scandal · Settled out of court	· Victim of espionage · Settled out of court
Main developments	· Known for adopting CI best practice · Develops CI business	· Known for adopting CI best practice	· Known for adopting CI best practice · Develops CI business	· Pioneers CI best practice	· Known for adopting CI best practice	· Known for adopting CI best practice
Main periods	· 1990s · Late 2000s (CI solutions for analytics/Big Data)	· Late 1990s	· 1990s · Late 2000s (CI solutions for analytics/Big Data)	· 1980s	· 1990s · Early 2000s	· Early 2000s
Actors	· CEO as initiator · Top management involved · Hires secret service veterans as experts; introduces standard CI practices (Herring 1996; 1999),	· CI units in R&D	· COO (CEO, President) Involvement · Hires CI experts; introduces standard CI practices · Decentralised CI units	· CEO as initiator · Hires generations of secret service veterans (e.g. CIA) to lead CI who standardize CI practices (Herring 1996; 1999)	· CEO involvement · Executives/former employees of competitors · Former Motorola CEO, pioneer of CI, joins P&G board · Hires secret service veterans (e.g. FBI) who standardize CI practices	· Top management involved · CEO/executives were employees of rivals
Practices & processes	· Focus on tech, R&D, rivals' new product launches extend to customers · Teams led by key executives · Emphasis on integration of IT, human CI network · CI part of strategic planning · common training/practices to protect CI and reputation	· Focus on technology patents grows to include consumer trends · Seek opportunities through CI · Alert other units · Sharing of CI	· Customer focus · Combining low-high tech · Executives centralise CI · CI (alliance ,newsgroups) · Feedback from customers by, e.g. executives in field · IT facilitates (networking, portals, dashboards)	· Focus on technology expands to broader environment · Emphasis of IT in CI · Human-source CI collection · Process of Management Needs Identification	· Focus on consumers and solutions extends to competitors · training to collect/protect intelligence, protect reputation · Sharing of CI via central CI unit · CI part of day-to-day purchasing · CI efforts cover partners, rivals, suppliers and employees	· training to collect/ protect intelligence, protect reputation · Patent tracking · Policies to protect CI · Random security/ scrutiny checks of employees
Structures	· Central unit with key executives leading decentralised efforts · Culture and team based	· Sub-unit of R&D department	· Decentralised structure · CI units directly linked to heads of departments and executives	· First corporate CI unit with dedicated people	· Corporate CI unit · Hub & spoke (real and virtual) · CI uses contractors and external locales ('the ranch', 'Kremlin')	· Decentralised, consensus-style
Key similarities	· Develops standard CI · Sees CI as inevitable · Keeps low visibility of CI · Supplies CI solutions	· Develops standard CI · Keeps low visibility of CI	· Develops standard CI · Sees CI as inevitable · Keeps low visibility of CI · Supplies CI related solutions	· Pioneers standard CI practice · Sees CI as inevitable · Keeps low visibility of CI	· Develops standard CI · Sees CI as inevitable · Keeps low visibility of CI	· Develops standard CI · Sees CI as inevitable · Keeps low visibility of CI

Table 3.2: Cross Case Analysis (Intel, Oracle, Texas Instruments and Unisys)

Company (CI association)	**Intel** (high)	**Oracle** (high)	**Texas Instruments (TI)** (high)	**Unisys** (high)
Antecedents	· Japanese competition · Settled out of court	· CI scandal · Settled out of court	· Victim of espionage · Settled out of court	
Main developments	· Known for adopting CI best practice · Develops as supplier to CI industry	· Known for adopting CI best practice · Develops CI business	· Known for adopting CI best practice	· Known for adopting CI best practice · Develops CI business
Main periods	· 1980s · Early 2000s (develops position as supplier to CI related industries)	· 1990s · Late 2000s (CI solutions for analytics/Big Data)	· Late 1990s	· 1990s · Early 2000s (develops CI products and solutions as part of security industry)
Actors	· CEO as initiator · Hires secret services veterans as experts; introduces standard CI practices · CI department led by ex-CIA officer	· CEO involvement, emphasis on customer feedback · CI function	· CEO as promoter · Hires generations of secret service veterans (e.g. CIA) to lead CI who standardize CI practices (Herring) · CI from within R&D and tech focus to firm	· CEO changes focus of CI · Business unit R&D CI staff · CI from internal focus on R&D and tech to focus to support corporate strategy process
Practices & processes	· Focus on monitoring of rivals' R&D, technology expands to include clients · Increasing centralisation · Intelligence sharing · Integrating CI processes · Fact based decisions	· Focus on technology/ markets expands to clients/ rivals · Increasing centralisation · Incentives to share CI · Intelligence sharing · Continuous feedback from customer contact · Intranet for sharing	· Focus on technology and R&D expands to market and rivals · Increasing centralisation · Increases incentives for cross unit sharing of CI · Introduces formal CI training · Structured CI processes · System support	· Focus on rivals' technology expands to customers · Increasing centralisation · Increasing focus on online threat · Develops communities of practice for knowledge sharing · Acquisition of key supplier to US CI community
Structures	· Multiple CI units · CI for strategic planning · Dashboard environment	· Established in R&D · Later centralised CI function and database	· Establishes CI within R&D · Strategy Leadership Team creates central CI	· Establishes central CI unit · Strategic alliance with government funded (CIA) intelligence firm
Key similarities	· Develops standard CI · Sees CI as inevitable · Keeps low visibility of CI · Supplies CI providers	· Develops standard CI · Sees CI as inevitable · Keeps low visibility of CI unit · Supplies CI related solutions	· Develops standard CI · Keeps low visibility of CI unit	· Develops standard CI · Keeps low visibility of CI unit · Supplies CI related solutions

Table 4.1: Factors of Persistence

Abstraction from Raw Data	Categories and Themes	Key Concepts
Victim of industrial espionage. Surprise with negative outcomes (speed of change, digitalisation, crisis). CEO insider to Intelligence Community. Key external professionals hired or involved (e.g., J. Herring, CIA (1996; 1999)). Intelligence function established. External experts actively gather information globally. Focus on experts' processes, tools. Sophisticated (IT) tools/simple routines (e.g., communities of professionals) are linked to business opportunities.	**Emergence (antecedents of adoption)** Trauma of victimisation (through transgression by others). Surprise by crisis. Aiming for best practice (i.e., model of professionalism, e.g., government unit).	**Opaqueness** Perception of existing best practice as better kept secret. Simplicity (e.g., dumpster diving). Lack of transparency (even for internal CI experts). Demand for non-observability (ability to keep the practice under the radar). Professional behavioural routines and professional skills lead to persistence. Seeking of settlements.
Increasing scope of practice (serving more disciplines; corporate level). CEO/Chairman /new executives emphasise key role of CI for corporate strategy. CEO establishes CI (e.g., set up squad of CI teams led by senior executives with professional support by same/similar experts, integrates Knowledge Management, intelligence processes and technology). CI training (compulsory) for all employees to enhance professional capabilities. Cross unit sharing of customer and competitor information. Gathering and analysing intelligence on targeted market segments. Focus on competitors' R&D expands to include broader environment. R&D and marketing work closely together and share intelligence. Supports corporate strategy process, decision making and sales force. Communities of practices and reward systems to motivate employees to conduct CI activities.	**Diffusion** Increasing scale and scope Commitment of senior executives Expertise and the adoption of professional tools to fulfil perceived needs (e.g., revenge, protection, survival, competitive advantage). Direct involvement of top management. Hiring of CI experienced professionals.	

Table 4.2: Factors of Persistence

Abstractions from Raw Data	Categories and Themes	Key Concepts
Led from corporate level. Focus on Key Intelligence Topics (modelled on US Government's approach). Professionalization ("best practices"). Specialisation (within corporation or departments). From decentralisation to centralised structure. Integration of separated databases. IT a multiplier for CI (e.g. Dynamic modelling of competition). Key analytical group with diverse members. Cross-functional teams. Professional intelligence network. Establishment of professional body to support the CI profession. Development of professional code of conduct. Broad anticipation of threats. Key CI consultants, Herring (formerly CIA) and Gilad, join forces in late 1990s and merge with Fuld to form Academy of Competitive Intelligence Violations and victimisation. Scandals and law suits. Actors infiltrate competitors and focal company teams and departments to identify leaks. Targeting competitors' consultants, suppliers, customers and employees. Surveillance, "regular inspections", by security department teams lead by former FBI agent. Zealous, regular and random checks of internal security and employees. Global multi-sector, cross-country threats of CI activities (e.g., moles). Careers in CI. CI advisors, consultants and professionals. Moving from public to private intelligence functions. Internal CI career ladder. Part-time CI careers. Routinized reactions to scandals. Scapegoating. Personnel changes. Out-of-court settlements. Public announcements and pledges.	**Formalisation and Standardisation** Standardisation across industry, Competitive parity, firm-level similarities in conducting CI, doing the same thing. **Transgressions and Reputational Damage** Covert activities may go unnoticed (embarrassment for victims) Transgressions can lead to a scandals (shaming of perpetrators) **Diversification and Damage Control** Growing numbers and diversity in CI community. Differentiation. Scandals and transgressions resolved quietly backstage. Few cases brought forward after 1996 Espionage Act.	**Constructing Usefulness and Invoking Fear** Leveraging strong beliefs about the need for CI. Motivating specific CI routines. Invoking fear about unilateral abandonment. **Practice Adaptation** Impression management that seeks association of CI practice with what is legitimate and dissociation with what is not.

[i] Penenberg and Barry (2000) speak of the "Intelligencing of Corporate America" and Warrell and O'Murchu (2013), and Evans (2013) report on many blue chips among more than 100 companies in the City of London that deploy CI practices.

[ii] A former Vice President at Lancome and L'Oreal emphasises the non-rational, intuitive dimension of CI and the difficulties of gauging its effectiveness (Salmon and de Linares 1999).

[iii] Estimates of the size of the CI market range from US$1-2 billion a year worldwide. Over 25% of the 520 CI practitioners worldwide (Competitive Intelligence Foundation, 2006) said their company's total CI spending in 2000 surpassed $100,000, and 14% said their company spent over $500,000 on CI or CI-related activities (Calof and Wright, 2008). One benchmarking report found the average CI operating budget of more than twenty firms to be $821,613 with large variance (Business Wire, 2006). Overall, Firms engaging in CI spend on average 1% of their revenue on CI (Pfaff, 2005).

[iv] A search in Google reveals the lack of information on CI. For example, searching for company "IBM" together with "marketing" ("accounting"; "logistics") generates 124 (46; 16) million hits. The joint results for "competitive intelligence" amount only to 2 million hits. While many academic journals are dedicated to marketing, logistics, or accounting, few are dedicated to competitive intelligence.

[v] While we relied for the selection on databases and specifically the Wall Street Journal, we broadened our sources to get a richer picture of CI in relation to the companies. We included data from (1) newspapers (e.g., Wall Street Journal, New York Times); (2) magazines (e.g., Business Week, Fortune, Forbes, Harvard Business Review, Journal of Business Strategy, Journal of Information Security, Journal of Marketing Intelligence and Planning, Strategy & Leadership); (3) trade journals (e.g., Advertising Age, Chief Executive, Computerworld, Electronic Business, International Business, Management Services, Marketing Tools, Research Technology Management, Review of Business and Technology, Software Magazine); (4) archival company data, such as annual reports and press releases available through online company databases and websites; (5) professional literature on CI; (6) conversations with practitioners and professionals.

[vi] We are grateful to the editor and reviewer's guidance to extend the period of observation.

[vii] After the collapse of the Soviet Union, a large number of CI professionals appeared on the job market, which made finding experienced talent easier than during times of high governmental demand for such expertise.

[viii] For additional interview quotes on CI' emergence, diffusion and persistence and Practice Persistence see Appendix 3.

[ix] The Society of Competitive Intelligence Professionals (SCIP) founded by a leading CI consultant seeks to enhance "the success of our members through leadership, education, advocacy, and networking" (www.scip.org) and provides a code of conduct that excludes any activities that might cause scandals.

[x] A controversial "employee-retention effort" "inside the CIA allows serving officers to moonlight in the private sector during their off hours" (Houston *et al*., 2012).