Chapter 10
The Global Click Fraud Industry

"Computer-based detection gives the defender economies of scale, but the attacker can use those same economies of scale to defeat the detection system" (Schneier, 2009).

"Cybercriminals used to be individual hooligans showing off their prowess, but the fact that it is so profitable, so easy to do and comparatively low-risk has made cybercrime an extremely attractive felony and, as a result, it has mushroomed into a giant global industry that is unlikely to stop growing anytime soon," Maxim Shirokov, Kaspersky Lab's regional director for the Middle East and Africa (cf. Naidu, 2008).

Abstract Click fraud is arguably the cyberworld's biggest scam. How do click fraudsters frame their actions? What are the characteristics of click fraud victims? How do formal and informal institutions affect click fraudsters' actions? We address these questions by examining the contexts, mechanisms, and processes associated with the click fraudsters' profitability and performance. We also discuss some attempts to criminalize and stigmatize click fraudsters.

10.1 Introduction

Click fraud is pervasive and is arguably the cyberworld's biggest scam (Agarwal, Athey, & Yang, 2009; Arnott, 2008). Illegitimate and unwanted clicks on paid advertisements have raised the ire of advertisers and rekindled debate about the effectiveness of online advertising. Cyber-criminals involved in diverse activities such as online pornography and software piracy are capturing potential economies of scope and are expanding their operations into lucrative businesses in the search advertising industry. Search engine network partners, competitors, and unhappy employees are receiving financial and psychic benefits from their engagements in generating illegitimate clicks. In 2004, Google's chief financial officer noted: "Click fraud is the biggest threat to the Internet economy" (Veverka, 2006).

A related, but less well-known phenomenon is impression fraud, in which ads are placed on invisible web pages and are not presented to Internet users. Such ads

N. Kshetri, *The Global Cybercrime Industry*, DOI 10.1007/978-3-642-11522-6_10,

are opened when an Internet user visits a website (Leggatt, 2009). It is reported that advertisers such as Kraft Foods, Greyhound, and Capital One have fallen victim of such a scam. In this chapter, we examine the contexts, mechanisms, and processes associated with the click fraud industry.

10.2 Clicks and Value Creation in the Internet Economy

As an advertising medium, part of the fascinating character of the Internet stems from its measurability and instant feedback. The basic idea behind search advertising and pay per click (PPC) model is simple: From a marketer's standpoint, a genuine click represents the clicker's personal choice, which provides an opportunity to create and deliver value and make money (Cart, 2000). Businesses are thus understandably willing to invest in generating clicks to attract consumers (Cell I, Table 10.1).

The Internet's measurability, which is a driving force behind the rapid growth of online advertising, is however, more complicated than first meets the eye. As illustrated in Table 10.1, a click does not necessarily represent the clicker's interest in the product, service, or content. Some websites pay people for clicking on ads or typing certain words into search engines. Some sites also run forums to exchange click fraud tips (Kehaulani, 2006). These fraudulent clicks arise from a malicious intent of a user to make an advertiser pay for unwanted and invalid clicks (Cells II and IV, Table 10.1), which have raised the question of infallibility of the Internet's measurability. In Parker's (1976, 17–21) typology of computer crimes, click fraud thus involves a computer as the "instrument" of the offense as well as its "symbolic"

Table 10.1 Click and value creation in the Internet economy

Value created⇒ Payment ⇓	Positive	Zero
Paid clicks	[I] • Genuine click on ads distributed by a PPC provider • Paying to *create positive brand* value through consumer-generated contents	[III] • Bogus and fake clicks (human- or machine-generated) on ads distributed by a PPC provider
Free clicks	[II] • Managing user-generated content to *create positive brand* value	[IV] • Advertisers and providers agree as "garbage traffic" or an invalid click

representation. This last point may warrant elaboration. In click frauds, computers are used symbolically to "deceive or defraud victims" (Parker, 1976). That is, click frauds "rely partially on the perceived infallibility of computer-generated information" (Hollinger & Lanza-Kaduce, 1988, p. 103).

Advertisers and search providers differ widely in their assessment of the proportion of clicks that belong to Cell III and IV in Table 10.1. PPC providers such as Google and Yahoo maintain that invalid clicks that are not proactively detected (Cell III, Table 10.1) account for less than 0.02% of total clicks. Advertisers think that this proportion is higher and argue that PPC providers' secretive techniques to detect invalid clicks have held them at bay.

Faced with massive click frauds, advertisers have challenged the infallibility and reliability of click-related data. There have been legitimate arguments about whether the current approach of measuring and counting clicks and identifying invalid clicks is equitable. Attacking the symbolic basis of PPC, advertisers have complained that search providers such as Google and Yahoo have not taken enough measures to protect them from illegitimate clicks and have provided tacit support for click fraud activities (Leonard, 2006).

To move to a different issue, some companies pay to generate clicks on consumer-generated contents (Cell III, Table 10.1). However, critics are concerned about manipulation of consumer reviews and paid reviews (Sullivan, 2008). China's public relations (PR) firms such as Daqi.com, Chinese Web Union, and CIC charge US $500–25,000 monthly to monitor online postings for a business. They help minimize the impact of negative information and create positive brand value for the company. There are reports that these PR firms hire college students to write good postings about certain brands and to criticize the competition (Roberts, 2008). In other cases, traffics on consumer-generated contents (e.g., reviews on products or the company) may result in actionable sales leads, for which businesses do not pay (Cell III, Table 10.1). There is increasing evidence to suggest that user-generated content, consumer-generated product reviews, and word-of-mouth are beginning to shape consumers' perception of a company and its offerings (Clemons, 2008). Indeed, consumer-generated Internet content is increasingly displacing other media (Martin & Smith, 2008). One estimate suggested that about a third of the top 300 retail websites offer consumer-generated reviews (Sullivan, 2008). Most consumers, however, do not realize that they could be charging for the contents they produced (Cart, 2000).

10.3 A Survey of Click Fraud

Consumers are increasingly relying on the Internet for information search. In 2007, Internet users worldwide conducted 61 billion searches per month (Burns, 2007). In December 2008, Americans conducted 12.7 billion online searches (Sullivan, 2009). Businesses are gearing up to respond to this surge in online searches. The global

Internet advertising was worth US $27 billion in 2006 and is expected to reach US $61 billion by 2010 or 20% of total ad spending (The Economist, November 25, 2006). An estimate suggested that about 40% of all Internet ads belong to the PPC category (Kehaulani, 2006). In 2006, advertisers worldwide spent US $15 billion on PPC advertising (Epstein, 2007). One estimate suggests that US businesses will spend US $12.3 billion in online search advertising in 2009 (Emarketer, 2009). Google dominates the PPC business. The company had a 61.2% share of searches in October 2008 compared with 16.9% for Yahoo and 11.4% for Microsoft (USA Today, December 17, 2008).

Studies vary as to the size of the problem as the proportion of fraudulent clicks is difficult to quantify. Estimates of fraudulent clicks as a proportion of total clicks vary from 10 to 50% (Mann, 2006). Most academics and consultants who study online advertising estimate that 10–20% of ad clicks are fake (Table 10.2). Others put it at 30% (Lynn, 2006). Automated scripts or computer programs are being increasingly used by click fraudsters to generate fake and bogus clicks, which imitate a legitimate user clicking on an ad (Table 10.2).

Estimates suggest that the United States and Canada account for as much as 90% of click frauds (Gonsalves, 2006; Utter, 2006). Top click fraud originating countries outside North America include India, China, Russia, the UK, France, Germany, Monaco, and Ghana (Table 10.2). Networks of human clickers engaged in click fraud are also reported to operate from former Soviet Union economies, South Africa, Bulgaria, Czech Republic, Egypt, Ukraine, Botswana, Mongolia, Vietnam, Honduras, Syria, and others (Chapell, 2006; Einhorn, 2006; Marketing, 2006; Vidyasagar, 2004; Grow, Elgin, & Herbst, 2006, Lynn, 2006; Motlogelwa, 2007). Some website owners have formed international networks to click on ads on each other's sites. One such network, Mutualhits.com, was reported to have over 2,000 members in 2006 (Kehaulani, 2006). Recent surge in click frauds are also associated with and facilitated by parked sites. These sites have little or no content except for Internet ads supplied by search providers such as Google and Yahoo.

Click fraudsters mostly target the US online advertising industry. However, click fraud's footprints across the world economy are getting bigger. In South Korea, there were over 134 million cases of click fraud in the first three quarters of 2006. Click frauds accounted for 11% of clicks on ads provided by Overture Korea in the first 9 months of 2006 (chosun.com, 2006). Likewise, the market research firm Analysys' survey in China conducted in 2006 indicated that one-third of respondents believed they had been click fraud victims (Einhorn, 2006).

As is the conventional world's shadow economy (Dillman, 2007), many legitimate actors are knowingly or unknowingly tied to click frauds. Legitimate Internet advertisers are indirectly funding click fraud activities. An estimate suggested that in 2004 advertisers paid over US $1 billion for spyware placements (Edelman, 2007). In 2007, a New Zealand-based hacker admitted his involvement in secretly installing the Dutch company, ECS International's adware on computers. He reportedly earned more than US $36,000 for this work (Gleeson, 2008). In another case, a Bot herder group in California, which pled guilty to a hospital hack, earned more than US $100,000 in affiliate advertising income.

Table 10.2 Some click fraud-related indicators

Year	Study conducted by	Fraudulent clicks as a proportion of total clicks	Top click fraud originating countries outside North America	Remarks
2005	Yankee group	10%		Click frauds cost advertisers US $500 million (PPC ads generated $5 billion)
2006Q1	ClickForensics	13.7%	China and France	Tier 1 search providers: 12.1%, Tier 2: 21.3%, Tier 3: 29.8%
2006Q2	ClickForensics	14.1% (20.2% for higher-priced ads)	India (increased by 26% during the quarter)	Higher-priced ads > $2 per click
2007Q1	ClickForensics	14.8% (22.2% for higher-priced ads)		Botnets accounted for about 9% of all click frauds
2007Q4	ClickForensics	16.6%	India (4.3%), Germany (3.9%), and South Korea (3.7%)	Botnets accounted for 22% of all click frauds
2008Q1	ClickForensics	16.3%	Monaco and Ghana: (each 3.1%).	Botnets accounted for 23.5% of all click frauds
2008Q2[a]	Click fraud network	16.2%	China (4.3%), Russia (3.5%), France (3.2%)	Botnets accounted for 25% of all click frauds
2008Q4	ClickForensics	17.1%		Botnets accounted for over 31.4% of all click frauds (compared to 27.6% in 2008Q3)

[a] Higgins (2008).

10.4 A Click Fraudster's Cost–Benefit Calculus

As noted in Chap. 2, economists consider financial as well as psychic costs and benefits to analyze individuals' propensity to engage in criminal activities. Equation 2.1 in Chap. 2 is specified to capture the behavior observed in an individual criminal. Nonetheless, the logics associated with the parameters can be extended at the firm level to investigate the firm's engagement in click fraud activities or incentives to discourage them. For instance, O_{cm} can capture a firm's potential reputation damage for engaging in click fraud. Likewise, P_a in Eq. 2.1 (Chap. 2) can be mapped with the probability of click fraud detection. In this section, we examine the parameters of Eq. 2.1 by analyzing the characteristics of offenders and victims associated with click frauds as well as institutions in which they are embedded.

10.4.1 The Offenders

10.4.1.1 Reputation, External Visibility, and Measures to Prevent Click Frauds

Click fraud rates vary across ads provided by various search providers. For instance, click fraud rates for Tier 1 search providers (e.g., Yahoo and Google) are higher than those for Tier 2 providers (e.g., Ask, MSN, Lycos) and Tier 3 ones (e.g., Dogpile) (Table 10.2). Google also offers three choices to advertisers: (1) advertising on Google.com only, (2) Google.com and major search partners such as AOL and AskJeeves, and (3) Google.com and the network of its affiliates. Click fraud rates are the highest in (3) and the lowest in (1) (Vise, 2005). Likewise, a study by China IntelliConsulting found that Baidu had a click fraud rate of 34%, compared to Google's 24% in China (Greenberg, 2007). In 2006, a Beijing hospital claimed that Baidu directed a scheme in which one of its affiliates maliciously generated fake clicks on the hospital's ads (Barboza, 2006).

Click fraud rates thus tend to be higher for ads involving less visible players. Why might this be the case? One reason behind a higher click fraud rates for ads distributed by smaller search providers, distributors, and affiliates may be that they are less likely to be spotlighted by the media. To examine why firms show a differential tendency to engage in and respond to potentially demeaning and reputation-damaging activities such as click fraud it would be helpful to consider the stigmatization process associated with such activities. A central concept here is *arbiters*. Wiesenfeld, Wurthmann, and Hambrick (2008) argue that arbiters' "constituent-minded sensemaking" influences the stigmatization process. Wiesenfeld et al. (2008) have identified three categories of "arbiters"—social, legal, and economic. Social arbiters include members of the press, governance watchdog groups, academics, and activists. Legal arbiters are those who enforce rules and regulations. Economic arbiters make decisions about engaging in economic exchange with individuals.

The media reports serve as an intermediary affecting the perceptions of market audience about a firm's scandalous and "nonconforming" behaviors (Rindova, Pollock, & Hayward, 2006). Media reports have played a critical role in the criminalization of computer crimes (Hollinger & Lanza-Kaduce, 1988).

Prior research indicates that the extent to which arbiters and other external actors criticize, devalue, or question a firm following a reputation-damaging event is a function of the firm's external visibility and reputation (Rhee & Valdez, 2009). In the automobile industry, for instance, media are more likely to target and write negative comments on recalls by higher reputation automakers than on by higher reputation automakers (Haunschild & Rhee, 2004; Rhee & Haunschild, 2006). Consistent with theory, search providers with a higher degree of external visibility seem to direct more efforts toward preventing click frauds. In 2006, Yahoo announced that the company developed a technology for collecting "traces" of Internet advertising users' paths (Leonard, 2006). The technology did not require to record Internet users' data. In 2006, Google launched a feature for advertisers to see the invalid clicks detected by the company (Los Angeles Times, 2006). That may be a small comfort for online advertisers. Google has sued click fraudsters and credited advertisers when click fraud is detected.

10.4.1.2 Hypermediation and Click Fraud

A central feature of the Internet economy is a near zero transaction cost. An emerging body of literature asserts that business is undergoing hypermediation as opposed to disintermediation, as some analysts had suggested (Cart, 2000). New intermediaries have emerged to provide services such as aggregating, matching suppliers and customers, providing trust, and providing inter-organizational market information (Bailey & Bakos, 1997).

The roots of the click fraud lie partly in this hypermediation. An increase in the number of sub-distributors increases the probability of click frauds. Portals and PPC providers such as Yahoo and Google do not normally disclose the chain of intermediaries involved in online advertising. Identifying them from outside is difficult. To understand hypermediation-led click frauds, consider one detail. It was found that a Vonage ad passed through layers of eight sub-distributors and was "illegally" downloaded to users' PCs (Businessweek.com, April 24, 2006). Likewise, an online ad of Dell, which was carried by Yahoo in 2005 was sent to distributor InfoSpace, which was then delivered to Direct Revenue. Direct Revenue put the ad in a pop-up (Elgin, 2006).

In the early days, PPC ads were displayed only as Search Engine results pages. PPC was thus called Search Engine advertising. The PPC syndication networks can be viewed as intermediaries, which match advertisers with relevant audience (Bailey & Bakos, 1997). In some cases, the PPC syndication networks are a better match than Search Engine results pages and provide high-conversion rates at low CPCs (Epstein, 2007).

Site owners of programs such as Google's AdSense, Yahoo's Publisher Network, or other contextual networks earn a part of the PPC charge for clicks on ads generated on their sites. Ad network partners, for instance, accounted for at least 30% of Google's revenue in 2008 and were paid about 25% of the company's revenue as commissions (Perez, 2009).

The hypermediation in the online search industry has acted as a crime generator by bringing potential click fraudsters in the value chain of the industry. PPC syndication networks consist of players with different sizes, reputations, and external visibility. A Google "help" page entitled "Where will my ads appear?", for instance, mentions brand names such as AOL.com and New York Times (Grow et al., 2006). In the early 2005, Google's AdSense program had about 200,000 websites consisting of individual bloggers, small businesses, and other websites (Graham, 2005).

We noted above that a firm's external visibility is negatively related to its engagement in reputation-damaging activities such as click fraud. Following this logic, we can argue that small sub-distributors and small Adsense affiliates are more likely to engage in click fraud-related activities compared to websites with higher external visibility such as AOL.com and New York Times. The publishers and search engine network partners benefit directly from click frauds. They have an incentive to develop creative ways to click on ads on their websites. Note too that these site owners lack external visibility and thus are less likely to be targeted by media.

10.4.1.3 The Economic Geography: Locations of Click Fraud Operations

It is tempting to employ low-wage workers from developing countries to generate clicks on ads, and collect commission from PPC programs. As noted above, most search terms cost just US $0.10—0.15 per click. Let's assume that it takes 8 seconds for an individual to click on an ad and view a page and the advertiser has to pay US $0.10 to a PPC provider for the click. At this rate, the clicker's activities generate US $45 per hour. Even if we assume that PPC providers and other intermediaries involved in click fraud activities take 90% of this amount, the clicker can still make US $4.50 per hour. This amount is much higher than many people make in developing countries. Declining connectivity and computer costs have made this a reality. There are reports that housewives, college graduates, and working professionals in India make US $100–200 per month by clicking on Internet ads (Vidyasagar, 2004).

The low-wage workers, however, may face an entry barrier if advertisers and PPC engines activate geo-targeting and monitor traffic originated from unusual geographical locations. Note that search engines allow an advertiser to choose the countries it would like to target and offer services related to IP address filtering (Mello, 2006). For instance, Overture South Korea's "continental cut-off" services block clicks from Africa (chosun.com, 2008).

A country's size of the online advertising industry is positively related to the attractiveness of click fraud activities generated in the country. The US, for instance, has the world's biggest online advertising industry. In 2008, about half of Google's revenue came from the United States (Perez, 2009). Unsurprisingly, suppliers pay

more for adware installs in a US computer compared to those in other countries. Adware suppliers such as the Dutch firm E.C.S. International reportedly paid 30 cents for each install in the United States (Businessweek.com, April 24, 2006). The rates for non-US machines were: 20 cents for Canada, 10 cents for the UK, and 1–2 cents in most other countries (Espiner, 2007).

10.4.1.4 Economics of Labor versus Technology and Technological Economies of Scope

Click fraudsters are also confronted with the problem of whether to employ the seemingly bottomless source of human clickers in developing countries or technologies enabling click fraud. In this regard, it is important to note that most organizations take a reactive approach to click fraud. Click fraud-enabling technologies are developing more rapidly than anti-click fraud technologies developed according to advertisers' reactive decisions (Matin, 2007). For instance, spyware is used to generate pop-up ads (Robertson, 2006). Fraudsters also use automated clicking models such as "Hitbots" or "Clickbots" (Graham, 2005).

As noted above, advertisers and PPC providers employ mechanisms such as geo-targeting and IP address filtering to detect click frauds. In such cases, botnet generated click frauds are more effective as they are less detectable compared to those associated with click fraud farms (Perez, 2009). Botnet generated click frauds come from a large numbers of home computers that are geographically distributed and have unique IPs and hence mimic legitimate clicking behavior. Algorithms used by PPC providers and third-party auditors, which look for unusual traffic patterns, thus may fail to identify botnet generated click frauds. From the click fraudster's standpoint, click fraud-enabling technologies may reduce the proportion of defective products. Click fraud-enabling technologies can be viewed as process innovations, which change the production process, leading to a higher level of "quality" (Standing, 1984). They can also be viewed as improvement innovations, which help "extend a branch of industry" and reduces production costs (Standing, 1984; p. 128).

Consumers are duped by "free" software, video games, and pornography. For instance, Easycracks.net, the Armenia-based company, which describes itself as "one of the biggest cracks database on the internet" and boasts itself as having "a complete list of cracks, serials, nocds patches and keygens" (www.easycracks.net). Easycracks lures consumers by offering free download of unauthorized copies of Windows XP and video games, which also requires the installation of ECS International's software, ActiveX controls. When users approve the installation, 16 other pieces of adware are downloaded to the user's machine without permission, which delivers up to five pop-up ads per minute (Businessweek.com, April 24, 2006).

Economies of scope exist if a technology is used in a variety of activities. For instance, easycracks describes itself as "a site for all your software needs." Botnets, which were mainly used to perpetrate spam in the past, is being used for click fraud (Mindlin, 2008). According to Click Forensics, in the second quarter of 2008,

botnets accounted for more than a quarter of all click frauds. Cyber-criminals have used botnets to fraudulently increase traffic to specific online ads and generate false clicks in massive numbers. For instance, the KMeth worm targeted Yahoo! Messenger users. The worm directed infected users to a website hosting Google AdSense ads related to mesothelioma (Leyden, 2006).

Online pornographers are turning to the click fraud industry. For instance, Internet users are lured to click on naked pictures, which takes them to a legitimate site and registers as a click (Mello, 2006). Note that the PPC model is based on the premise that each click represents a personal choice. In such a case, the clicker actually visited the advertiser's website without an interest to do so.

10.4.1.5 Economic and Psychic Benefits of Wasting Competitor's Ad Budget

There are economic and psychic benefits (satisfaction) associated with wasting a competitor's advertising budget. Some illegitimate and malicious clicks are funded by companies to waste their competitors' online ad budgets (Marketing, 2006). There have been arrests related to such frauds (Zaharov-Reutt, 2008).

Businesses usually have limits on how much they would spend on PPC advertising. Once they reach the limit, search engines do not display their ads. Pushing competitors' links off the search sites help the fraudsters ads receive a higher priority for the keyword search and are displayed more prominently (Matin, 2007). Such frauds thus mainly victimize small businesses with limited budget in competitive spaces with PPC costs. Some also benefit psychically from wasting a competitor's advertising budget. Psychologists refer this phenomenon as enjoyment-based intrinsic motivation (Deci & Ryan, 1985). Olsen (2004) reported that the chief executive of an Internet marketing company enjoyed clicking on his competitors' ads on Google and Yahoo. The executive said that clicking on competitors' ads is "an entertainment."

Many companies have reported that they have suffered from competitor-generated bogus clicks on their ads. The Atlanta-based insurance company, MostChoice.com reported that its ads were clicked by competitors (Vise, 2005). Likewise, Karaoke Star reported that one of its competitors employed an automated click fraud program to target Karaoke Star and other online Karaoke stores (Penenberg, 2005). Similarly, JetNetwork, a charter-jet service in Miami Beach, claimed that over 40% of the clicks on the company's ads came from a single IP address belonging to a rival (Mann, 2006).

10.4.1.6 Institutions and Click Fraud

Institutional perspective thus can help us understand complex causes and roots associated with click fraud. It is important to note that institutional theory is described as "a theory of legitimacy seeking" (Dickson & BeShers, 2004, p. 81). To gain legitimacy, organizations adopt behaviors irrespective of the effect on organizational efficiency (Campbell, 2004, p. 18). Institutional influence on the click fraud industry thus becomes an admittedly complex process when organizations have to derive legitimacy from multiple sources such as the state, trade and professional

Table 10.3 Institutional mechanisms associated with criminalizing and stigmatizing click frauds

Level of institutions	Mechanisms	Remarks/examples
National/state	• *Adoption of statutes* and regulations addressing click frauds	• Click fraud is a felony covered by Penal code 502 in California and the Computer Misuse Act 1990 in the United Kingdom
	• Strengthening cybercrime-related rule of law	• 2007: 17 US states had adopted statutes *to* deal with spyware (Skrzycki, 2007)
Industry, trade/professional associations	• Codes of ethics require members to maintain higher standards of conduct than required by law	• Direct Marketing Association's *guidelines* for software downloading
		• The Click Measurement Working Group launched by the Interactive Advertising Bureau (IAB)
Inter-organizational	• *Economic exchange-related* responses	• 2006: A coalition of brands such as Expedia and LendingTree pressured Google and Yahoo to be more accountable (Grow et al., 2006)
		• 2006: A group of advertisers, including PepsiCo, Hewlett-Packard, and Kimberly-Clark demanded audited numbers and common measurement standards (Leonard, 2006)
Intra-organizational	• *Intra-organizational rules, norms*, and culture to deal with click frauds	• 2005: Priceline.com started working on a draft of the company's adware policy (Heun, 2005)
Individual	• Feeling of guilt or remorse	• Many clickers in developing countries click on ads just to make money and do not know that some *businesses are victimized* by their activities

associations, business partners, and individuals. These institutions thus exist at various levels (Table 10.3), which affect financial and psychic costs and benefits in equation (2.1, Chap. 2) by attacking the ingredients and ecosystems of click frauds and influencing factors such as arrest, stigma, and earnings associated with (McCarthy, 2002).

10.4.1.7 Regulative/Formal Institutions and Click Fraud

In nascent and formative sectors such as Internet advertising, there is no developed network of regulatory agencies comparable to established industrial sectors (Powell, 1993). Governments are adopting statutes and regulations to deal with click frauds.

For instance, click fraud is considered as a felony in some economies. As of 2007, there was no federal law prohibiting spyware in the United States. Nonetheless, many states had adopted statutes to deal with spyware, which is used to generate pop-up ads (Skrzycki, 2007).

Law-enforcement agencies are also beginning to take a closer look at click fraud and criminalize associated activities. In the United States, the Securities and Exchange Commission (SEC) filed fraud charges in 2005 against operators of 12dailypro.com, which allegedly operated a pay-to-read advertising (Kehaulani, 2006). In September, 2006, a cybercrime unit led by the FBI and US Postal Inspection Service assigned analysts to examine possible violation of federal laws by click frauds. The Senate Judiciary Committee has launched its own informal probe (Grow et al., 2006). In the same year, a federal grand jury also indicted a Pennsylvania man for allegedly operating a click fraud network (Kehaulani, 2006).

Countries with weak rule of law and permissiveness of regulatory regimes have provided a fertile ground for click fraud activities (Mittelman & Johnston, 1999; Vassilev, 2003). In the United States, the FBI acted on after the agency noticed suspected cyber-criminals discussing click frauds in secret chat rooms (Grow et al., 2006). In India, on the other hand, companies openly advertised in national newspapers looking for people, who would use home computers to click on Internet ads (Kehaulani, 2006). To return to the Easycracks.net and ECS International example above, ECS International was prosecuted for engagement in cybercrimes thanks to the Netherlands' strong cybercrime laws (Gleeson, 2008). Easycracks.net is, however, likely to be safer because of Armenia's weak enforcement of such laws (Giragosian, 2006, 2007). Higher-level institutions and exogenous parameters have thus been favorable to Easycracks.net (Snidal, 1994, 1996).

Because of low-opportunity costs of conviction and low values of P_a and P_c because of weak law-enforcement measures, the expected penalty (O_{cm}, P_a, P_c) in Eq. (2.1) of engaging in click fraud is low in developing countries such as India and Armenia.

10.4.1.8 Informal Institutions and Click Fraud

Edelman and Suchman (1997) note: "the legal rules 'cause' the organizational practices (or vice versa) is, at best, a gross simplification." Anti-click fraud norms and practices are evolving at the industry, inter-organizational, and intra-organizational levels to deal with click frauds and to criminalize and stigmatize such activities.

In prior literature, researchers have noted professional and trade associations constitute the "most elaborate and intricate organizational arrangements" (Scott, 1992, p. 253) and play a significant role in legitimating institutional changes (Greenwood, Suddaby, & Hinings, 2002, Kshetri & Dholakia, 2009). For instance, trade and professional associations have codes of ethics, which require members to maintain higher standards of conduct than required by law (Backoff & Martin, 1991). The Direct Marketing Association issued guidelines, which require marketers to give clear and conspicuous notice to consumers to download software and an easy way

to uninstall it (Skrzycki, 2007). In 2006, the Center for Democracy and Technology asked the Federal Trade Commission to take action against an adware company, which repeatedly and intentionally attempted to trick Internet users into downloading intrusive software (Chabrow, 2006). In August 2006, the Interactive Advertising Bureau (IAB) launched The Click Measurement Working Group to create a set of Click Measurement Guidelines. Members include search vendors such as Yahoo, Google, Microsoft, and Ask.com, and industry body the Media Rating Council (MRC) (IT Week, 2006). In South Korea, small-scale online businesses have established the Online Advertisers Association, which has voiced concerns click fraud (chosun.com, 2008).

To understand inter-organizational relations, it may be helpful to consider the roles of economic arbiters, which make economic exchange-related decisions. In this regard, advertisers are actively mobilizing discourses against technology and service providers to take anti-cybercrime measures. In the United States, advertisers have pressured Google and Yahoo to be more accountable and have demanded audited numbers and common measurement standards (Grow et al., 2006; Leonard, 2006). Inter-organizational relations are also shaped by broad "macro-cultural discourse" and associated institutions, which extend beyond the boundaries of the business (Berger & Luckmann, 1967; Lawrence & Phillips, 2004). Search engines in China do not face such pressures and thus tend to be more lenient on click fraud (Lu, 2007).

An important question is: Do click fraudsters have a feeling of guilt or remorse for engaging in click frauds? As discussed earlier, most of those who make unethical uses of computer networks may not perceive their actions' ethical implications. For instance, many clickers in India click on ads just to make money and do not know that some businesses are victimized by their activities. Social identity theory also points to the possibility of ethnocentric bias (Hamner, 1992; Tajfel & Turner, 1986). This means that the level of perceived guilt is smaller for out-group victims than for ingroup ones.

10.4.2 The Victims

10.4.2.1 Profiles of Click Fraud Victims and Targets

Prior research indicates that crime opportunity is a function of target attractiveness, which is measured in monetary or symbolic value (Clarke, 1995). To put things in context, two observations are worth making regarding the targets of click fraud. The first observation is that return to click fraud or the monetary benefit (M_b in 2.1, Chap. 2) is positively related to the price of a search term. As noted above, site owners of programs such as Google's AdSense, Yahoo's Publisher Network or other contextual networks earn a percentage of the PPC charge for every click on ads on their sites. While some search terms cost just 10–15¢ per click, others cost several hundred dollars. Search terms related to law, medicine, finance, and travel

industries are among the most expensive ones (Liptak, 2007). For instance, in 2005, for "D.C. Hair Laser Removal," maximum cost per click was US $146 and average cost per dick was US $69 (Penenberg, 2005). Most obviously, companies that buy higher-priced search terms are more likely to fall victim of click fraud (Milyan, 2007).

Second, to avoid detection, click fraudsters are more likely to target companies that buy more terms (Matin, 2007). Advertising networks and third-party auditors employ various methods to identify invalid clicks. The method perhaps most often utilized entails identifying clicks that significantly deviate from the past clicking history. Likewise, according to rules-based algorithms, a click is considered as invalid if click fraud filters identify "specific conditions or a series of conditions" defined by the algorithms (Matin, 2007, p. 542). If different keywords bought by a competitor are searched, instead of a single term, fraudulent clicks could be considered as legitimate competitor analysis and research.

10.4.2.2 Poorly Protected Computers and Weakness of Defense Mechanisms

Click frauds have mainly victimized advertisers. It would be erroneous, however, to assume that advertisers are the only victims of click fraud. Note too that weakness of defense mechanism co-varies positively with the likelihood of becoming a crime victim (Glaeser & Sacerdote, 1999). Consumers are both instrument and victim of click fraud schemes. Other things being equal, naive users' poorly protected computers are more susceptible to such schemes. Their compromised computers are infested with annoying pop-up ads and are also used as vehicles to perform click fraud. For instance, in 2005, the Russian website, iFrameCash.biz exploited a Microsoft Windows security hole to distribute adware products. Microsoft promptly patched the hole. Many computers around the world, however, remained vulnerable for a long time (Anderson, 2008).

Internet users in developing economies are attractive targets for botnet generated click frauds. As discussed in Chap. 8, in developing countries, many Internet users connected to the Internet for the first time are not security oriented (Information Today, 2008; redherring.com, 2005).

10.4.2.3 Preventing Click Fraud: The Cost–Benefit Calculus

Prior research indicates that individuals and organizations can reduce the probability of becoming crime victims and losses by buying insurance policies or by using safety measures such as anti-burglar systems and safety deposit boxes, or by living in safe neighborhoods (Ehrlich & Becker, 1972). From a potential victim's perspective, the cost–benefit calculus associated with preventing click fraud activities involves determining the optimum investment as well as types of measures needed (Anderson & Schneier, 2005). For small companies, identifying fraudulent clicks may be a challenge. Tools such as Click Lab, Click Defense, and Click Detective are available to identify fake and bogus clicks. Such tools, however, cost from

US $30 to several thousand dollars per month (Penenberg, 2005). Click frauds are especially painful and frustrating for small companies, which are overwhelmed by search engine marketing budgets and thus are forced to accept fraudulent clicks as a cost of doing business.

10.5 Concluding Comments

Click fraud has been an uncomfortable reality facing the search advertising industry and has posed a threat to the growth of this industry. The presumed infallibility of click measurement is eroding because of massive click frauds. We examined the contexts, mechanisms, and processes associated with the click fraudsters' profitability and performance.

Various groups of arbiters are providing legal, ethical, and economic pressures to firms associated with click fraud. They are directing efforts toward criminalizing and stigmatizing click frauds, which may change the fraudsters' cost–befit calculus. The above analysis indicates that the roots of click frauds lie partly in asymmetric hypermediation consisting of a dense network of organizations in the supply side such as PPC providers, sub-distributors, and affiliates; and thin and dysfunctional institutions to perform trust-producing roles.

The above discussion also indicates that advertisers need to be vigilant about click fraudsters' creative ways to increase profitability. They need to take measures to minimize victimization. As noted above, the differences in click frauds can be partly explained by differing reputation levels of the players involved in the value chain of Internet advertising. There is thus a complex trade-off between minimizing victimization by paying a higher rate to search providers with a high degree of external visibility or accepting a higher click fraud rate with less reputed search providers. Small companies that cannot afford tools to identify fake and bogus clicks may look for unusual clicking behavior and regularly track conversion rates to see whether their PPC ads are working.

Many analysts argue that anti-click fraud actions of Yahoo and Google are only symbolic, which are designed to appease the advertisers and thus lacked substantiveness. PPC providers' anti-click fraud measures thus need to be driven by substantive considerations. Well-coordinated, well-funded campaign can create the perception of infallibility, validity, and reliability of PPC information, and reassure advertisers that their ad dollars are effectively spent. We noted above the emergence of new intermediaries to match suppliers and customers. Increasing pervasiveness of click frauds has also created a compelling need for new types of intermediaries. Establishment of intermediaries to provide a third-party measurement system capable of producing trust may address some of the concerns in the search advertising industry.

Finally, businesses need to direct more efforts toward harnessing the power of consumer reviews, blogs, and other forms of online endorsement as an alternative to PPC advertising. Most often, these are less costly, relatively fraud free, and are becoming more effective. While practices such as hiring consumers to write good

things about a company and manipulation of consumer reviews have ethical implications, businesses can find ethical ways to manage consumer-generated contents. For instance, according to Amazon.com's conditions of use statement, the company reserves "the right (but not the obligation)" to edit or remove user-generated content.

References

Agarwal, N., Athey, S., & Yang, D. (2009). Skewed bidding in pay-per-action auctions for online advertising. *American Economic Review, 99*(2), 441–447.

Anderson, M. (2008, July 2008). Crimeware pays: Adware, phishing, and spam are a strange—and big—business. *IEEE Spectrum.* http://www.spectrum.ieee.org/jul08/6375. Accessed 2 October 2008.

Anderson, R., & Schneier, B. (2005). Counterpane internet security guest editors introduction: Economics of information security. *IEEE Security & Privacy, 3*(1), 12–13.

Arnott, S. (2008, March 22). Cyber crime stays one step ahead. http://www.independent.co.uk/news/business/analysis-and-features/cyber-crime-stays-one-step-ahead-799395.html. Accessed 2 October 2008.

Backoff, J. F., & Martin, Jr., C. L. (1991). Historical perspectives: Development of the codes of ethics in the legal, medical and accounting professions. *Journal of Business Ethics, 10*, 99–110.

Bailey, J. P., & Bakos, Y. (1997). An exploratory study of the emerging role of electronic intermediaries. *International Journal of Electronic Commerce, 1*(3), 7–20.

Barboza, D. (2006, September 17). The Rise of Baidu (That's Chinese for Google). http://www.nytimes.com/2006/09/17/business/yourmoney/17baidu.html?pagewanted=3&_r=1. Accessed 2 October 2008.

Berger, P. L., & Luckmann, T. (1967). *The social construction of reality: A treatise in the sociology of knowledge*. New York: Doubleday.

Burns, E. (2007, October 15). Worldwide Internet: Now Serving 61 Billion Searches per Month Search Engine Watch. http://searchenginewatch.com/3627304. Accessed 2 October 2008.

Businessweek.com. (2006, April 24). Your ad here. And here. And here. http://www.businessweek.com/magazine/content/06_17/b3981046.htm. Accessed 2 October 2008.

Campbell, J. L. (2004). *Institutional change and globalization.* Princeton, NJ: Princeton University Press.

Cart, N. G. (2000). Hypermediation: Commerce as Clickstream. *Harvard Business Review, 78*(1), 46–47.

Chabrow, E. (2006). The spies inside. *InformationWeek, 1082*, 34–40.

Chapell, A. (2006, October 13). Re-evaluating click fraud. http://www.imediaconnection.com/printpage/printpage.aspx?id=11361. Accessed 2 October 2008.

Chosun.com. (2006, October 31). Click fraud sets back internet advertising. http://english.chosun.com/w21data/html/news/200610/200610310025.html. Accessed 2 October 2008.

Chosun.com. (2008, July 15). Online advertisers demand industry reforms.

Clarke, R.V. (1995). Situational crime prevention. In Tonry, M. & Farrington, D. P. (Eds.), *Building a safer society. Strategic approaches to crime* (pp. 91–150). Chicago: University of Chicago Press.

Clemons, E. K. (2008). How information changes consumer behavior and how consumer behavior determines corporate strategy. *Journal of Management Information Systems, 25*(2), 13–40.

Deci, E. L, & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behavior*. New York: Plenum Press.

Dickson, M., & BeShers, R. G. V. (2004). The impact of societal culture and industry on organizational culture: Theoretical explanations. In R. J. House, P. J. Hanges, M. Javidan, P. W. Dorfman, & V. Gupta (Eds.), *Culture, leadership, and organizations: The GLOBE study of 62 societies*. Thousand Oaks, CA: Sage Publications.

Dillman, B. (2007). Introduction: Shining light on the shadows: The political economy of illicit transactions in the Mediterranean. *Mediterranean Politics, 12*(2), 123–139.
Edelman, B. (2007, January 25). Why I can never agree with adware and spyware. *The Guardian*.
Edelman, L. B., & Suchman, M. C. (1997). The legal environments of organizations. *Annual Review of Sociology, 23*, 479–515.
Ehrlich, I., & Becker, G. (1972). Market insurance, serf-insurance and serf-protection. *Journal of Political Economy, 80*(4), 623–648.
Einhorn, B. (2006). Advertisers in China are getting burned, too. *Business Week, 4003*, 54.
Elgin, B. (2006). Yahoo's pop-up connection. *Business Week*, July 17 (3993), 45.
Emarketer. (2009, February 6). US Search Ad Spending Falters? http://www.emarketer.com/Article.aspx?id=1006902. Accessed 2 October 2009.
Epstein, A. J. (2007, April 23). Online merchant's guide to pay per click advertising. *AuctionBytes.com*. http://www.auctionbytes.com/cab/abn/y07/m04/i23/s03. Accessed 2 October 2008.
Espiner, T. (2007, December 14). Cracking open the cybercrime economy. *ZDNet News*. http://news.zdnet.com/2100-1009_22-180416.html. Accessed 2 October 2008.
Giragosian, R. (2006). Redefining Armenian national security. *Demokratizatsiya, 14*(2), 223–234.
Giragosian, R. (2007). Armenia on the move: A comparative assessment. *AGBU, 17*(1), 22–24.
Glaeser, E. L., & Sacerdote, B. (1999). Why is there more crime in cities? *The Journal of Political Economy, 107*(6), 225–258.
Gleeson, S. (2008, April 2). Superhacker convicted of international cyber crime. http://www.nzherald.co.nz/category/story.cfm?c_id=30&objectid=10501518. Accessed 2 October 2008.
Gonsalves, A. (2006, April 24). Click fraud less than expected. *Monitoring Firm Says*. http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=186700544. Accessed 2 October 2008.
Graham, J. (2005, November 3). Google's AdSense a bonanza for some websites. *USA Today*.
Greenberg, A. (2007, July 3). More Evil than Google? http://www.forbes.com/2007/07/03/google-evil-competition-tech-techbiz-cx_ag_0703googevil.html. Accessed 2 October 2008.
Greenwood, R., Suddaby, R., & Hinings, C. R. (2002). Theorizing change: The role of professional associations in the transformation of institutionalized fields. *Academy of Management Journal, 45*(1), 58–80.
Grow, B., Elgin, B., & Herbst, M. (2006). Click fraud. *Business Week, 4003*, 46.
Hamner, K. M. (1992). Gay-bashing: A social identity analysis of violence against Lesbians and Gay Men. In G. M. Herek & K. Berrill (Eds.). *Hate crimes: Confronting violence against Lesbians and Gay Men* (pp. 179–90). Newbury Park, CA: Sage.
Haunschild, P. R., & Rhee, M. (2004). The role of volition in organizational learning: The case of automotive product recalls. *Management Science, 50*, 1545–1560.
Heun, C. T. (2005). Can spyware ever come in from the cold? *InformationWeek, 1061*, 70–71.
Higgins, K. J. (2008, July 28). Botnets behind one fourth of click fraud. *DarkReading*. http://www.darkreading.com/security/government/showArticle.jhtml?articleID=211201369.
Hollinger, R., & Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws. *Criminology, 26*, 101–126.
Information Today. (2008). *Challenges in the East, 25*(2), 22.
IT Week. (2006, August 14). Advertising body fights click fraud, 13.
Kehaulani, S. (2006, October 22). 'Click Fraud' threatens foundation of web ads; Google faces another lawsuit by businesses claiming overcharges. *The Washington Post*, A.1.
Kshetri, N., & Dholakia, N. (2009). Professional and trade associations in a nascent and formative sector of a developing economy: A case study of the NASSCOM effect on the Indian offshoring industry. *Journal of International Management, 15*(2), 225–239.
Lawrence, T. B., & Phillips, N. (2004) From Moby Dick to Free Willy: Macro-cultural discourse and institutional entrepreneurship in emerging institutional fields. *Organization, 11*, 689–711.

Leggatt, H. (2009, October 13). Online advertisers duped by 'invisible' ads. *BizReport*. http://www.bizreport.com/2009/10/online_advertisers_duped_by_invisible_ads.html. Accessed 27 October 2009.

Leonard, D. (2006). When is a click not a click? *Fortune, 154*(5), 53.

Leyden, J. (2006, October 6). Worm automates Google AdSense fraud. . http://www.theregister.co.uk/2006/10/06/google_adsense_worm. Accessed 2 October 2008.

Liptak, A. (2007, October 15). Competing for clients, and paying by the click. *The New York Times*. http://www.nytimes.com/2007/10/15/us/15 bar.html. Accessed 27 October 2009.

Los Angeles Times. (2006, August 3). In brief/internet; Search engines unite to fight 'Click Fraud', C.4.

Lu, P. B. (2007, March). CIC China search engine advertisers survey brief 1Q2007. http://www.researchinchina.com/headline/download/ChinaPaidSearchAdvertisersSurvey1Q2007.pdf. Accessed 2 October 2008.

Lynn, M. (2006, October 7). Why Google has already passed its peak. *The Spectator*.

Mann, C. C. (2006, January). How click fraud could swallow the internet. *WIRED Magazine, 14*(1). http://www.wired.com/wired/archive/14.01/fraud.html. Accessed 27 October 2008.

Marketing. (2006, July 19). Media analysis: Click fraud rears its head. http://www.accessmylibrary.com/coms2/summary_0286-33091453_ITM. Accessed 2 October 2008.

Martin, K. D., & Smith, N. C. (2008). Commercializing social interaction: The ethics of stealth marketing. *Journal of Public Policy & Marketing, 27*(1), 45–56.

Matin, S. (2007). Clicks Ahoy! Navigating online advertising in a sea of fraudulent clicks. *Berkeley Technology Law Journal, Annual Review, 22*(1), 533–554.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology, 28*, 417–442.

Mello, J. P. Jr. (2006, May 1). Pornographers turn to click fraud. *E-Commerce Times*. http://www.ecommercetimes.com/story/48135.html. Accessed 2 October 2008.

Milyan, A. (2007, May 14). Developing click fraud standards: Q&A with Tom Cuthbert l Click Forensics. http://www.searchmarketingstandard.com/articles/2007/05/developing-click-fraud-standards-qa-with-tom-cuthbert-l-click-forensics.html. Accessed 2 October 2008.

Mindlin, A. (2008, June 16). Rogue computers used in ad fraud; [Business/Financial Desk]. *New York Times,* (Late Edition (East Coast)), C.4.

Mittelman, J. H., & Johnston, R. (1999). The globalization of organized crime, the courtesan state, and the corruption of civil society. *Global Governance, 5*(1), 103–126.

Motlogelwa, T. (2007, October 5). Cyber crime law gets teeth. http://www.mmegi.bw/index.php?sid=1&aid=30&dir=2007/October/Friday5. Accessed 27 October 2009.

Naidu, E. (2008, May 11). Cybercrime expert comes to SA. http://www.iol.co.za/index.php?set_id=1&click_id=139&art_id=vn20080511082218330C406913 Accessed 1 October 2008.

Olsen, S. (2004, July 19). Exposing click fraud. *CNET News*. http://news.cnet.com/Exposing-click-fraud/2100-1024_3-5273078.html. Accessed 2 October 2008.

Parker, D. B. (1976). *Crime by computer*. New York: Charles Scribners' Sons.

Penenberg, A. L. (2005). So many clicks, so few sales. *Inc, 27*(8), 29–30.

Perez, J. C. (2009, January 26). Google Q4 earnings plummet, revenue up 18%. http://www.techworld.com.au/article/274113/google_q4_earnings_plummet_revenue_up_18. Accessed 2 October 2009.

Powell, W. W. (1993). *The social construction of an organizational field: The case of biotechnology*. Paper presented at the Warwick-Venice workshop on Perspectives on Strategic Change, University of Warwick.

redherring.com. (2005, April 5). China's Zombie PCs. http://www.redherring.com/Home/11708. Accessed 2 October 2008.

Rhee, M., & Haunschild, P. R. (2006). The liability of good reputation: A study of product recalls in the US automobile industry. *Organization Science, 17*, 101–117.

Rhee, M., & Valdez, M. E. (2009). Contextual factors surrounding reputation damage with potential implications for reputation repair. *Academy of Management Review, 34*(1), 146–168.

Rindova, V. P., Pollock, T. G., & Hayward, M. L. A. (2006). Celebrity firms: The social construction of market popularity. *Academy of Management Review, 31*, 50–71.
Roberts, D. (2008). Inside the war against China's Blogs; Vengeful bloggers? Flaming posts? PR firms help global brands navigate the country's perilous Web. *Business Week, 4089*, 60.
Robertson, B. (2006, October 23). China's Internet Mess; Search-engine firms routinely use spyware to capture market share. Now they face allegations of click fraud. *Newsweek* (International ed.)..
Schneier, B. (2009, October 15). Why framing your enemies is now virtually child's play. *The Guardian*. http://www.guardian.co.uk/technology/2009/oct/15/bruce-schneier-internet-security. Accessed 22 October 2008.
Scott, W. R. (1992). *Organizations: Rational, natural and open systems*. Englewood Cliffs, NJ: Prentice Hall.
Skrzycki, C. (2007). Stopping Spyware at the source. *The Washington Post*, D.1.
Snidal, D. (1994). The politics of scope: Endogenous actors, heterogeneity and institutions. *Journal of Theoretical Politics, 6*(4), 449–472.
Snidal, D. (1996). Political economy and international institutions. *International Review of Law and Economics, 16*(1), 121–137.
Standing, G. (1984). The notion of technological unemployment. *International Labour Review, 123*(2), 127–147.
Sullivan, E. A. (2008, February 15). Consider your source. *Marketing News, 42*(3), 16–19.
Sullivan, L. (2009, February 6). Brick-and-Mortar retailers losing search battle. *MediaPost*. http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=99829. Accessed 2 October 2008.
Tajfel, H., & Turner, J. C. (1986). The social identity theory of intergroup behavior. In S. Worchel & W. G. Austin (Eds.), *Psychology of intergroup relations* (pp. 7–24). Chicago, IL: Nelson-Hall.
The Economist. (2006). *Leaders: Truth in advertising; Internet commerce, 381*(8505), 12.
USA Today. (2008, December 17). Marketers hone the focus of search ads.
Utter, D. A. (2006). High-priced keyword click fraud rises. http://www.webpronews.com/insiderreports/2006/07/17/highpriced-keyword-click-fraud-rises, July 17. Accessed 2 October 2008.
Vassilev, R. (2003). De-development problems in Bulgaria. *East European Quarterly, 37*(3), 345.
Veverka, M. (2006). How Click Fraud Just Got Scammier; Calling All "Bot" Busters!. *Barron's*, 44.
Vidyasagar, N. (2004, May 3). India's secret army of online ad 'clickers'. http://timesofindia.indiatimes.com/articleshow/msid-654822,curpg-1.cms. Accessed 2 October 2008.
Vise, D. A. (2005). Clicking to steal: When advertisers pay by the look. *The Washington Post*, F01. http://www.washingtonpost.com/wp-dyn/articles/A58268-2005Apr16.html. Accessed 2 October 2008.
Wiesenfeld, B. M., Wurthmann, K. A., & Hambrick, D. C. (2008). The stigmatization and devaluation of elites associated with corporate failures: A process model. *Academy of Management Review, 33*(1), 231–251.
Zaharov-Reutt, A. (2008, November 30). Click fraud: Advertisers to watch closely. *ITWire*. http://www.itwire.com/content/view/21990/53. Accessed 28 October 2009.