The Economics of Click Fraud

By: Nir Kshetri

Kshetri, Nir (2010) "The economics of click fraud", IEEE Security & Privacy, 8 (3), May/June, 45-53.

Abstract:
Click fraud is a substantial threat in the cyberworld. Here, the author examines the contexts, mechanisms, and processes associated with the click-fraud industry from an economics viewpoint. The nature of electronic channels, characterized by asymmetric hypermediation, provides a fertile ground for such fraud.

Click fraud is arguably the cyberworld's biggest scam. Illegitimate clicks on pay-per-click (PPC) advertisements have rekindled debate about online advertising's effectiveness. Cybercriminals involved in diverse activities are expanding their operations into lucrative businesses in the PPC industry. At the heart of the click-fraud problem is the fact that site owners benefit from clicks made to ads on their sites. Search engine network partners, competitors, and unhappy employees can all generate illegitimate clicks. Here, I examine the contexts, mechanisms, and processes associated with the click-fraud industry from an economics viewpoint.

Article:
Clicks and Value Creation in the Internet Economy
As an advertising medium, one fascinating character of the Internet stems from its measurability and instant feedback. In this regard, the basic idea behind the PPC model is simple: from a marketer's standpoint, a genuine click represents the clicker's choice, which provides an opportunity to create and deliver value. [1] Businesses are understandably willing to invest in generating genuine clicks.

However, the Internet's measurability, which is a driving force behind PPC advertising's growth, is more complicated than first meets the eye. As Table 1 presents, a click doesn't necessarily add value because not all clicks represent clickers' interest in the product or service. On the other hand, not all clicks need be paid to create value. In this article, I focus mainly on fake and invalid clicks (cells 3 and 4 in the table), but looking at the other types of clicks should help us better understand the click-fraud phenomenon.

Table 1. Click and value creation in the Internet economy.

Payment	Positive value created	Zero value created
Paid clicks	(1) Genuine clicks; paid consumer-generated content that creates positive value	(3) Fake clicks (human- or machine-generated) on ads the PPC provider distributes
Free clicks	(2) Unpaid user-generated content that creates positive value	(4) Clicks advertisers and providers agree are invalid

Positive Value, Paid by Advertisers
A genuine click on a paid ad, which represents the clicker's choice and lets the advertiser create and deliver value, falls in cell 1. Some companies have followed a different but related approach, which entails paying to create consumer-generated content. A *Business Week* article reported that China's public relations firms, such as Daqi.com, Chinese Web Union, and CIC, charge US$500 to $25,000 monthly to monitor online posts and help minimize the impact of negative information and create positive brand value for the company (June 2008;

http://tinyurl.com/3nopkd). According to the article, some reports say these firms hire students to write good posts about certain brands and criticize the competition. Critics are concerned about manipulation of paid consumer reviews.

Positive Value, Free to Businesses

Traffic to unpaid consumer-generated content can result in sales leads businesses don't need to pay for (cell 2). [1] Many businesses create and manage free networking sites, forums, and blogs to attract consumers. User-generated content, product reviews, and word of mouth are shaping consumers' perceptions and displacing traditional media. A *Marketing News* article observed that roughly a third of the top 300 retail websites offer consumer-generated reviews. [2]

No Value, Charged to Advertisers

Illegitimate clicks on PPC ads, for which advertisers get charged, fall in cell 3. Fraudsters use human and technological means to generate artificial clicks. Some publishers click on ads on their own websites, others pay a third party to do so, and still more use automated click-generating programs. As *The Washington Post* reported, click-exchange programs and forums exist to let site publishers exchange click-fraud tips (October 2006; http://tinyurl.com/ykksde). These fraudulent clicks arise from users' malicious intent to make advertisers pay, which raises questions about how infallible the Internet's measurability really is.

No Value, Advertisers Aren't Charged

PPC providers have developed techniques to detect fake clicks that provide no value, for which they don't charge advertisers (cell 4). A *Los Angeles Times* article explained that Google launched a feature that let advertisers see invalid clicks the company had detected (August 2006; http://tinyurl.com/27t24b9). Likewise, a *B&T Weekly* article [3] and a *Fortune* article (August 2006; http://tinyurl.com/28zbyss) reported that Yahoo's software could identify click fraud, allowing it to delete invalid click charges from advertisers' PPC accounts.

Advertisers and search providers differ widely in their assessment of how many clicks fall into cells 3 and 4. PPC providers such as Google maintain that invalid clicks that it doesn't proactively detect (cell 3) account for less than 0.02 percent of total clicks. [4] Advertisers such as Cars.com, Expedia, LendingTree, PepsiCo, Hewlett-Packard, and Kimberly-Clark believe that the proportion of undetected fraudulent clicks is higher and argue that PPC providers' secretive techniques to detect invalid clicks purposely keep them in the dark. Google, for instance, gives advertisers aggregated statistics but no information about whether it identified a particular click as valid or invalid.

A Survey of PPC Advertising and Click Fraud

According to searchenginewatch.com, Internet users worldwide conducted 61 billion searches per month in 2007 (October 2007; http://searchenginewatch.com/3627304), and *MediaPost* reported that in December 2008, Americans conducted 12.7 billion online searches (February 2009; http://tinyurl.com/cu7y7r). Businesses are gearing up to respond to this surge: the October 2006 *Washington Post* article noted that 40 percent of all Internet ads belonged in the PPC category. Estimates suggest that the proportion grew to 52 percent in 2007 and 57 percent in 2008. [4] PPC was the only form of Internet advertising that grew in 2008. AuctionBytes.com reported that in 2006, advertisers worldwide spent US$15 billion on PPC advertising (April 2007; http://tinyurl.com/26w96av), and Emarketer estimated that US businesses spent US$12.3 billion on such advertising in 2009. [5]

This increase in PPC advertising has implications for trends in click fraud. Table 2 presents some click-fraud indicators. Data from other available surveys don't differ significantly from the ones provided in the table. However, various security and consulting companies (listed in the second column) conducted these studies and could have vested interests in exaggerating the risks involved with click fraud. Fraudulent clicks as a proportion of total clicks (third column) are substantial and exhibit a somewhat increasing trend.

Table 2. Click-fraud-related indicators.

Year (*l*th quarter, *Ql*)	Study author	Fraudulent clicks as a proportion of total clicks (%)	Top click-fraud originating countries outside North America	Remarks
2005	Yankee Group	10		Click fraud cost advertisers US$500 million (pay-per-click ads generated $5 billion)
2006, Q1	ClickForensics	13.7	China and France	Tier 1 providers: 12.1% Tier 2: 21.3% Tier 3: 29.8%
2007, Q1	ClickForensics	14.8 (22.2 for higher-priced ads)		Botnets: 9% of click-fraud activities
2008, Q2	Click Fraud Network	16.2	China (4.3%), Russia (3.5%), France (3.2%).	Botnets: 25% of click-fraud activities
2008	Outsell[4]	13		

Studies vary as to the problem's size because methodological, logical, conceptual, and statistical problems make the proportion of fraudulent clicks difficult to quantify. Most academics and consultants estimate that 10 to 20 percent of ad clicks are fake (see Table 2). Anecdotal data related to companies' experiences also illustrate this problem. Click fraud represented 20 percent of NewCars.com's ad spending on Yahoo in 2007. [4]

Estimates (for example, from informationweek.com [April 2006; http://tinyurl.com/2cxgkm8] and webpronews.com [July 2006; http://tinyurl.com/24wgk3j]) suggest that the US and Canada account for 90 percent of click-fraud activities. Some surveys have reported the top click-fraud originating countries outside North America, which are listed in the fourth column of Table 2 . A review of articles published in outlets such as imediaconnection.com (October 2006; http://tinyurl.com/2brjnfb), *Business Week* (October 2006; http://tinyurl.com/nfmgzs), *Marketing Magazine*, *The Spectator*, [6] the Botswanian daily newspaper, *Mmegi*, [7] the Indian national newspaper, *Times of India* (May 2004; http://tinyurl.com/2ka5g), and *The New York Times* (May 2009; http://tinyurl.com/r76pb4) suggests that networks of human clickers engaged in click fraud operate from South Africa, Bulgaria, the Czech Republic, Egypt, the Ukraine and other former Soviet Union economies, Botswana, Mongolia, Vietnam, Honduras, Indonesia, Syria, and others. California-based Cars.com reported that a large number of clicks on its ads came from Bulgaria, Indonesia, and the Czech Republic, where the company had no businesses. [4]

Some website owners have reportedly formed international networks to click on ads on each other's sites. The *Washington Post* article from October 2006 claimed that one such network, Mutualhits.com, had more than 2,000 members. Click fraud is also associated with and facilitated by parked sites, which have little or no content except for ads that search providers supply.

Click fraudsters mostly target businesses in the US and other industrialized countries. However, click fraud's footprints are getting bigger. According to *Chosun*, a South Korean newspaper, South Korea experienced more than 134 million cases of click fraud in the first three quarters of 2006, and fraud accounted for 11 percent of clicks on ads from Overture Korea, a commercial search service. [8] Likewise, the market research firm Analysys's 2006 survey in China indicated that one-third of respondents believed they'd been click-fraud victims (see http://tinyurl.com/nfmgzs).

Many legitimate actors are knowingly or unknowingly tied to click fraud. According to an article in *The Guardian*, advertisers paid more than US$1 billion for spyware placements in 2004 (January 2007; http://tinyurl.com/2bntrem). In 2007, a New Zealand-based hacker admitted his involvement in secretly installing the Dutch company ECS International's adware on computers; a *New Zealand Herald* article noted that the hacker earned more than US$36,000 for this work (April 2008; http://tinyurl.com/29dalwp). Likewise, securityfocus.com reported in 2006 that a bot-herder group in California earned more than US$100,000 in affiliate advertising (www.securityfocus.com/brief/204).

Click-Fraud Detection

Detecting click fraud is a conceptually challenging task. We can classify invalid click-detection methods under three categories.

The *anomaly-based* (or *deviation-from-the-norm-based*) approach considers invalid clicks to be those that deviate significantly from normal predicted behaviors. It involves analyzing offline aggregate data related to day-to-day activities to capture normal behaviors and derive a model. Instead of defining an invalid click, this approach defines a normal click and determines whether other clicks vary widely from the normal one. Challenges associated with this approach include determining what comprises normal and how much deviation is significant.

The *rule-based* approach uses heuristics to classify valid and invalid clicks on the basis of specific conditions. For instance, if two successive clicks occur, the second click might be an invalid one. PPC providers can implement session tracking to track a series of requests from the same user across a given period. Alexander Tuzhilin maintains that if a rule considers a click to be valid, then the click is justifiable if the rule demonstrates that it can occur by means that aren't prohibited [7] (for example, the click wasn't generated using bots or a publisher didn't click on Google's ads on his or her own website) or has a positive probability of conversion (see http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf).

Finally, the *classifier-based* approach is purely operational and employs data mining classifier labels to detect invalid clicks. This approach is based on the assumption that past clicking behaviors predict future clicking behaviors. It carries out this labeling on the basis of past data about valid and invalid clicking activities. The approach assumes that an advertiser has past data, which classifies a click as valid or invalid with a certain level of confidence and doesn't consider the properties of valid or invalid clicks discussed in the previous approaches.

Cost-Benefit Analysis

Let's next look at a cost-benefit analysis for a click fraudster, a PPC provider, and an advertiser. These benefits and costs can be either immediate or delayed.

The Click Fraudster

Economists consider financial as well as nonfinancial or psychic costs and benefits to analyze individuals' propensity to engage in criminal activities. For a click fraudster, benefits might include monetary gain and returns as well as psychic benefits such as enjoyment. Monetary and psychic costs are functions of the probabilities associated with fraud detection, fines, arrest, and conviction. Psychic costs include guilty feelings or other emotional penalties, which are separate from the risks of arrest and conviction.

The PPC Provider

A PPC provider's revenue is directly related to the amount of PPC advertising sold. As mentioned previously, online advertising providers don't charge advertisers for clicks that the providers identify as invalid via their detection systems. So, those providers directly benefit from valid clicks and might have a vested interest in labeling more clicks as valid ones. In the short run, PPC providers such as Google and Yahoo benefit from the fraud their affiliates commit. However, if a provider is associated with fraud, it might suffer a decline in reputation and bear a cost in the form of fewer opportunities to serve advertisers in the future.

The Advertiser

An advertiser likes to receive high-quality clicks on its ads for the lowest cost. We can explain advertisers' difficulties in benefiting from Internet ads' measurability in terms of behavioral and technological factors. The first problem is the imperfect relationship between click-through rates and conversion rates. That is, a website visitor who clicked on an ad doesn't necessarily buy the advertised product. The second problem concerns a lack of built-in mechanisms to protect advertisers against click fraud. Such mechanisms count in the advertiser's cost-benefit analysis, so losses occur due to clicks on ads that have zero probability of conversion to a buyer.

From the advertiser's perspective, a cost-benefit analysis associated with preventing click fraud involves determining the optimum investment and types of measures. [9] For small companies, identifying fraudulent clicks is a challenge. According to an *Inc* magazine article, tools such as Click Lab, Click Defense, and Click Detective, which are available to identify fake clicks, cost up to several thousand dollars per month. [10] Click fraud is painful for small businesses, which are overwhelmed by marketing budgets and are forced to accept fraudulent clicks as a cost of doing business.

How Electronic Channels Affect Click-Fraud Economics

Cyberspace is huge. From the standpoint of criminal groups, it's attractive in part because it's characterized by less governance and weak rule of law. Electronic channels are thus susceptible to higher opportunism, which increases the possibility that a potential seller will use deception to deliberately create an information advantage.

To understand the real and perceived costs and benefits for various parties, we might want to distinguish technological information from market information. According to *Machlup*, technological information refers to "knowledge of the technology of the time" (Internet ad effectiveness and conversion rate) and market information is "knowledge of the markets" (for instance, various players involved in the PPC value chain and their reputation levels). [11] We can frame this distinction as opportunities for production and opportunities for exchange. [12]

This limitation of electronic channels, which is related to the absolute level of information about product quality (quality of clicks on an online ad, such as effectiveness and conversion), is referred to as technological uncertainty. This type of uncertainty results from the complexity of quality measurement and individuals' bounded rationality. That is, due to cognitive limitations, individuals might have difficulty assessing and interpreting the quality of products and services offered online. Most online advertisers might accept this unmeasurable quality related to technological uncertainty as "fate" or the "state of things." [12] The problem here is one of information distribution as regards product quality, in which potential traders (such as an advertiser or Google and Adsense website owners) possess different levels of information about click authenticity. The quality uncertainty issue in click fraud is more concerned with market uncertainty than technological uncertainty. The PPC advertising industry thus suffers from George Akerlof's "lemons problem," [13] which concerns buyers' inability to distinguish between honest and dishonest sellers or between low- and high-quality goods and increases the potential for adverse selection, moral hazard, and fraud. That is, advertisers can't determine if the PPC provider, subdistributors, or affiliates are lying, cheating, or acting dishonestly.

Reputation and External Visibility

Click-fraud rates vary across ads from various search providers. For instance, as Table 2 shows, click-fraud rates for Tier 1 search providers (such as Yahoo and Google) are lower than those for Tier 2 (for example, Ask, MSN, or Lycos) and Tier 3 providers (Dogpile). Despite higher click-fraud rates, some advertisers use Tier 2 or 3 providers because they're cheaper. According to an *Economist* article, Google handles more than 75 percent of search-related ads in the US. [14] It also offers advertisers three choices: Google.com only, Google.com and major search partners such as AOL and AskJeeves, and Google.com and the network of its affiliates. According to the July 2006 webpronews.com article, click-fraud rates were the highest in the third case and the lowest in the first. Likewise, a study by China IntelliConsulting found that China's search engine, Baidu, had a click-fraud rate of 34 percent compared to Google's 24 percent in that country. In 2006, a Beijing hospital claimed that Baidu directed a scheme in which one of its affiliates generated fake clicks on the hospital's ads.

In e-commerce, barriers to entry are low, which lets buyers and sellers of all sizes and reputation levels participate. One reason behind higher click-fraud rates for ads distributed by smaller search providers, distributors, and affiliates could be that these providers are less likely to be in the media spotlight. To examine firms' differential tendency to engage in and respond to potentially demeaning and reputation-damaging activities such as click fraud, it helps to consider the stigmatization process. A central concept here is arbiters:

Batia Wiesenfeld and her colleagues argue that the actions of social, legal, and economic arbiters influence the stigmatization process. [15]

Media reports serve as an intermediary affecting the market audience's perceptions about a firm's scandalous behaviors. 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. [16] Moreover, costs associated with lost reputation are higher for reputed firms.

Search providers with greater external visibility have directed some anti-click-fraud efforts. The August 2006 *Fortune* magazine article mentioned previously reported that Yahoo developed a technology for collecting "traces" of Internet users' paths. To maintain and protect their reputations, PPC providers have sought legal recourse against click fraudsters. As covered in *The Washington Post* (April 2005; http://tinyurl.com/2crrn7u) and other sources, in 2004, Google filed a lawsuit against Auctions Expert International, a Texas-based Internet company. Likewise, *E-Commerce Times* (June 2009; www.ecommercetimes.com/story/67353.html) and other sources reported that in June 2009, Microsoft filed a lawsuit against three Canadians over click fraud.

Hypermediation and Click Fraud

A central feature of the Internet economy is near-zero transaction costs. An emerging body of literature asserts that business is undergoing hypermediation as opposed to disintermediation. [11] New intermediaries have emerged to provide various services. Click fraud's roots lie partly in hypermediation, or an increase in the number of subdistributors. PPC providers don't normally disclose their chain of intermediaries, and identifying them from the outside is difficult. To understand hypermediation-led click fraud, consider this detail: it was reported in 2006 that a Vonage ad passed through eight subdistributors and was illegally downloaded to users' PCs. [17] Likewise, a *Business Week* article suggested that a Dell ad that Yahoo carried in 2005 was sent to InfoSpace, which then delivered it to Direct Revenue, which put the ad in a pop-up (July 2006; http://tinyurl.com/2b3r5hv).

PPC syndication networks are intermediaries that match advertisers with a relevant audience. In some cases, such networks are a better match than search engine results pages and provide high conversion rates at a low cost. Hypermediation, however, has acted as a fraud generator by bringing potential click fraudsters into the value chain. PPC syndication networks consist of players with different sizes, reputations, and external visibility. A *USA Today* article pointed out that, in 2005, Google's AdSense program had roughly 200,000 bloggers, small businesses, and other websites enrolled (March 2005; http://tinyurl.com/267cspg). Following the logic from the previous section, we can argue that small subdistributors and Adsense affiliates, which have low external visibility and reputation, are more likely to engage in click-fraud-related activities.

A Click Fraudster's Strategic Elements

I noted earlier that site owners can benefit from clicks made to ads on their sites. In addition, economic and psychic benefits are associated with wasting a competitor's advertising budget. An article in *Marketing* explained that how some illegitimate clicks are funded wastes competitors' ad budgets (July 2006; http://tinyurl.com/2av7haj). *ITWire* magazine reported on arrests related to such frauds (November 2008; www.itwire.com/content/view/21990/53/).

Businesses usually have limits on how much they'll spend on PPC advertising. Once they reach these limits, search engines stop displaying their ads. Pushing competitors' links off search sites would help fraudsters' ads receive higher priority. Such frauds mainly victimize small businesses with limited budgets, and some fraudsters benefit psychically from wasting a competitor's budget. Psychologists refer to this phenomenon as *enjoyment-based intrinsic motivation*. [18] A *CNET News* article commented on one chief executive of a marketing company who found clicking on competitors' ads to be "an entertainment" (July 2004; http://tinyurl.com/peoal5).

Many companies have reported victimization from competitor-generated bogus clicks on their ads. The *Washington Post*'s April 2005 story explained how competitors repeatedly clicked Atlanta-based insurance company MostChoice.com's ads, and, in the previously mentioned *Inc* magazine article, [10] Karaoke Star complained that one of its competitors employed automated programs to target the company and other Karaoke stores. Similarly, the January 2006 issue of *Wired* reported that more than 40 percent of clicks to the Miami-based JetNetwork's online ads came from a single IP address belonging to a rival (www.wired.com/wired/archive/14.01/fraud.html).

Economic Geography: Locations of Click-Fraud Operations

It's tempting to employ low-wage workers from developing countries to generate clicks on ads and collect commission from PPC programs. The May 2004 indiatimes.com article reported that housewives, college graduates, and professionals in India make US$100 to $200 a month by clicking on Internet ads.

When a PPC engine or advertiser deploys invalid-click detection methods, however, employing low-wage workers becomes less attractive. Such workers face an entry barrier if advertisers and PPC engines activate fraud-detection tools such as IP address filtering, geo-targeting, or monitoring traffic generated from unusual locations. For instance, according to *Chosun*, Overture South Korea's "continental cut-off" services block clicks from Africa. [19]

The online advertising industry's size is positively related to the attractiveness of click-fraud activities targeting a country. Unsurprisingly, suppliers pay more for adware installs on a US computer compared to those in other countries. ECS International reportedly paid US$0.30 for each install in the US, whereas the rates for non-US machines were $0.20 for Canada, $0.10 for the UK, and $0.01 to 0.02 in most other countries. [20]

Labor vs. Technology and Technological Economies of Scope

Click fraudsters must often decide whether to employ the seemingly bottomless source of human clickers in developing countries or use technology. Some analysts assert that click-fraud-enabling technologies are growing more rapidly than anti-click-fraud ones developed according to advertisers' reactive decisions. A *PC World* article quoted a Cisco Secure Consulting Services manager: "Once you build a better mousetrap, hackers build better mice" (July 2001; http://tinyurl.com/2ak4t7o). Additionally, Botnet-generated clicks come from large numbers of geographically distributed computers with unique IP addresses. Algorithms that PPC providers and third-party auditors use to look for unusual traffic patterns might thus fail to identify such clicks.

Cybercriminals have many ways of tricking unsuspecting Internet users. For instance, consumers are duped by free software, games, and pornography. Easycracks.net, an Armenian company, lures consumers by offering free, unauthorized downloads of Windows XP and games, but requires that consumers install ECS International's ActiveX controls. When users approve the installation, Easycracks.net causes 16 pieces of adware to download to their computers without permission and deliver five pop-up ads per minute. [17]

Economies of scope exist if a malicious technology is used for multiple activities. Botnets, for example, are used for mass spam distribution, key-logging, identity theft, denial-of-service (DoS) attacks, phishing, and spyware, but cybercriminals also use them to fraudulently increase traffic to online ads and generate false clicks. An article published in *The Register* documented how the KMeth worm targeted Yahoo Messenger users by reportedly directing infected users to a website hosting Google AdSense ads about mesothelioma (October 2006; http://tinyurl.com/2erocsl). Similarly, an *E-Commerce Times* article highlighted how online pornographers are turning to click fraud: Internet users are lured to click on a link when a fraudster plants a false impression of a naked person, which takes the user to a website to register a click (January 2006; http://tinyurl.com/27hjye4).

Target Attractiveness

Crime opportunity is a function of target attractiveness, which we measure via monetary or symbolic values. Two observations are worth making regarding click-fraud targets. First, returns for click fraud are positively

related to the search term price. Site owners using Google's AdSense, Yahoo's Publisher Network, or other contextual networks earn a percentage of the PPC charge for clicks to ads on their sites. Although some search terms cost US$0.10 to $0.15 per click, those related to the law, medicine, finance, and travel industries are expensive. For instance, the *Inc* magazine article "So Many Clicks, So Few Sales" stated that for "D.C. Hair Laser Removal," maximum cost per click was US$146 in 2005. [10] Companies that buy higher-priced search terms are more likely to fall victim (see Table 2).

Second, to avoid detection, click fraudsters are more likely to target companies that buy more terms. As noted earlier, advertising networks and third-party auditors employ various methods to identify invalid clicks. If a fraudster searches a competitor's different keywords instead of a single term, the detection method, such as a rules-based algorithm, could label a fraudulent click as legitimate competitor analysis and research.

Poorly Protected Computers and Defense Mechanism Weakness

Click fraud has mainly victimized advertisers, but it would be erroneous to assume that they're the only victims. Weakness in defense mechanisms covaries positively with the likelihood of becoming a crime victim, and consumers are both instruments and victims of click-fraud schemes. Naive users' poorly protected computers are more susceptible to such schemes—their computers are infested with pop-up ads used to perform click fraud. An article entitled "Crimeware Pays" in *IEEE Spectrum* explained how the Russian website iFrameCash.biz exploited a Microsoft Windows security hole to distribute adware in 2005 (July 2008; www.spectrum.ieee.org/jul08/6375/). Microsoft patched the hole, but many computers worldwide remained vulnerable for a long time.

Internet users in developing economies are attractive targets for botnet-generated frauds. In these economies, users are often connecting to the Internet for the first time in their lives and aren't security oriented. Moreover, security products are unaffordable or unavailable in their native languages.

Institutions' Effects on Cost-Benefit Analyses

Click fraudsters' activities fit squarely with what William Baumol called destructive entrepreneurship. [21] Baumol hypothesized that the extent of destructive entrepreneurship in a society is a function of the "relative payoffs" offered by the society's "rules of the game." Institutions capture these rules, which, according to Nobel Laureate Douglass North, include "formal constraints (rules, laws, constitutions), informal constraints (norms of behavior, conventions, and self-imposed codes of conduct), and their enforcement characteristics." [22]

As Table 3 demonstrates, institutions can add financial and psychic value or costs to various actors. The first column shows the sources from which institutions affect actors' behaviors, the second summarizes mechanisms associated with each source, and the third presents some examples.

Table 3. Institutional mechanisms associated with criminalizing and stigmatizing click fraud.

Level of institutions	Mechanisms	Examples
National/state	Statutes and regulations addressing click fraud; cybercrime-related rule of law	Click fraud is a felony covered by Penal Code 502 in California (November 2008; http://tinyurl.com/26hzsur) and the Computer Misuse Act of 1990 in the UK (http://tinyurl.com/5g2w3h).
		As of 2007, 17 US states had statutes to deal with spyware.
Industry group, trade/professional association	Codes of ethics that require members to maintain higher standards of conduct than the law requires; economic exchange-related responses	The Direct Marketing Association has guidelines for software downloading.
		The Interactive Advertising Bureau (IAB) launched the Click Measurement Working Group.
		In 2006, a coalition of brands such as Expedia and LendingTree pressured Google and Yahoo to be more accountable for click fraud, and a group of advertisers, including PepsiCo, Hewlett-Packard, and Kimberly-Clark, demanded audited numbers from PPC providers and common measurement standards on the quality and authenticity of clicks.
Organizational	Organizational rules, norms, and culture	In 2005, Priceline.com drafted adware policy.
Individual	Feelings of guilt/remorse	Many clickers in developing countries might not realize that they're victimizing businesses.

National/State Level

Nascent and formative sectors, such as Internet advertising, don't have a developed regulatory agency network. Governments are, however, adopting statutes and regulations to deal with click fraud, which would change the cost-benefit equation for fraudsters. Law enforcement agencies are looking more closely at click fraud and criminalizing associated activities. As reported in reuters.com, Priceline, Travelocity, and Cingular paid more than $30,000 each to New York state to settle charges that they employed secret adware that led to pop-up ads (January 2007; http://tinyurl.com/265e4cl). In the US, the Securities and Exchange Commission (SEC) filed fraud charges in 2005 against 12dailypro.com, which allegedly operated a pay-to-read advertising network (http://tinyurl.com/ykksde). In 2006, a cybercrime unit led by the FBI and US Postal Inspection Service assigned analysts to examine how click fraud might violate federal laws (http://tinyurl.com/nfmgzs), and, in the same year, a federal grand jury indicted a Pennsylvania man for operating a click-fraud network (http://tinyurl.com/ykksde).

Countries with weak laws provide fertile ground for click fraud. The October 2006 *Business Week* article mentioned previously discussed how the FBI took action after noticing click-fraud discussions in chat rooms, whereas the October 2006 *Washington Post* article reported that, in India, companies advertised in national newspapers looking for people willing to use home computers to click on ads, with no repercussions from authorities.

Industry Group, Trade/Professional Association Level

Trade associations perform two critical functions: interest representation and self-regulation. Associations, which mainly emphasize the former role, are considered pressure groups, whereas those focusing on the latter role are considered extensions of state power.

We can explain the activities of various groups and advertiser coalitions organized around the shared interest of minimizing click fraud via the interest-representation role. According to *Chosun*, South Korean small businesses established the Online Advertisers Association to voice concerns about click fraud. [19] Such a role involves directing efforts to mobilize discourse and pressuring PPC providers to change existing technological and institutional arrangements. In the US, advertisers pressured Google and Yahoo to be more accountable and demanded audited numbers and common measurement standards. We can consider these advertisers to be economic arbiters that make economic exchange-related decisions. Prior research indicates that institutional arrangements favor organized groups and actors compared to unorganized ones. Organized groups can thus act as economic arbiters more effectively.

The self-regulation role describes the Click Measurement Working Group (CMWG) that the Interactive Advertising Bureau (IAB) launched in 2006 to create click-measurement guidelines. Members include Yahoo, Google, Microsoft, Ask.com, and the Media Rating Council (MRC). From a self-regulation angle, industry groups and trade associations such as the CMWG have codes of ethics that require members to maintain higher standards of conduct than the law does. The norms, informal rules, and codes can create order by relying on a decentralized enforcement process that penalizes noncompliance. [22] These activities help maintain and protect members' reputations.

Finally, broad institutions shape interorganizational relations. According to a survey from researchinchina.com, search engines in China are less likely to face pressures and are arguably more lenient on click fraud (see http://tinyurl.com/23vffp5). One way to understand the China–US difference is to consider their experiences with modern capitalism. Many successful firms in mature market economies are guided by customer orientation and demonstrate their commitment to customer focus. Customers in these economies thus expect high-quality products and services and exhibit a low tolerance if businesses and suppliers don't fulfill their implicit and explicit commitments. In China's central plan-based economic system, economic activities obviously lacked customer orientation. Due to China's short history of modern capitalism, Chinese clients and customers are more likely to tolerate a low level of product and service quality and reliability.

Organizational Level

Some organizational-level rules have led to reduced click-fraud opportunities. Priceline.com—which, according to an *InformationWeek* article was among the top 10 spyware advertisers (October 2005; http://tinyurl.com/23685ea)—drafted a new adware policy aimed at stopping the company's pop-up ads that third-party distributors such as Claria, Direct Revenue, and eXact Advertising often place.

Individual Level

We can assess a fraudster's psychic costs in terms of guilty or remorseful feelings. Experts argue that most people who use computer networks unethically don't perceive their actions' ethical implications. [23] For instance, many clickers in developing economies might just click on ads to make money and don't know that they're victimizing businesses. This is a consequence of the hypermediation effect discussed earlier.

Click fraud has been an uncomfortable reality facing the search advertising industry and has posed a threat to this industry's growth. Click measurement's presumed infallibility is eroding due to massive click-fraud schemes.

Many argue that anti-click-fraud actions from Yahoo and Google are only symbolic and designed to appease advertisers and are thus insubstantial. PPC providers' anti-click-fraud measures thus need to be driven by substantive considerations. Well-coordinated, well-funded campaigns can create the perception that PPC information is infallible, valid, and reliable and can reassure advertisers that they're effectively spending their ad dollars. Additionally, a third-party measurement system that can engender trust might address such concerns.

Finally, as mentioned earlier, consumer-generated content might perform similar functions to paid clicks. Businesses could direct efforts toward harnessing the power of consumer reviews, blogs, and other forms of endorsement as an alternative to PPC advertising. Most often, these methods are less costly, relatively fraud free, and are becoming more effective.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.

References

1. N.G. Cart, "Hypermediation: Commerce as Clickstream," *Harvard Business Rev.*, vol. 78, no. 1, 2000, pp. 46–47.
2. E.A. Sullivan, "Consider Your Source," *Marketing News*, vol. 42, no. 3, 15 Feb. 2008, pp. 16–19.
3. M. Nguyen, "Online Giants 'Failing to Educate Market on Click Fraud,'" *B&T Weekly*, vol. 56, no. 2589, 2006, p. 4.
4. S. Hamner, "Pay-Per-Click Web Advertisers Combat Costly Fraud," *The New York Times*,12 May 2009; www.nytimes.com/2009/05/13/business/media 13adco.html.
5. "US Search Ad Spending Falters?" Emarketer.com, 6 Feb. 2009.
6. M. Lynn, "Why Google Has Already Passed Its Peak," *The Spectator*,7 Oct. 2006.
7. T. Motlogelwa, "Cybercrime Law Gets Teeth," *Mmegi Online*,5 Oct. 2007, www.mmegi.bw/index.php?sid=1&aid=30&dir=2007/ OctoberFriday5.
8. "Click Fraud Sets Back Internet Advertising," *Chosun*,31 Oct. 2006.
9. R. Anderson and B. Schneier, "Economics of Information Security," *IEEE Security & Privacy*, vol. 3, no. 1, 2005, pp. 12–13.
10. A.L. Penenberg, "So Many Clicks, So Few Sales," *Inc*, vol. 27, no. 8, 2005, pp. 29–30.
11. F. Machlup, *The Production and Distribution of Knowledge in the United States*, Princeton Univ. Press, 1962.
12. A.H.J. Wurth, "Policy Information or Information Policy? Information Types in Economics and Policy," *Knowledge & Policy*, vol. 5, no. 4, 1992/93, pp. 65–81.
13. G.A. Akerlof, "The Market for 'Lemons': Qualitative Uncertainty and the Market Mechanism," *Quarterly J. Economics*, vol. 84, 1970, pp. 488–500.
14. "Clash of the Clouds," *Economist*, vol. 392, no. 8653, 2009, pp. 80–82.

15. B.M. Wiesenfeld, K.A. Wurthmann, and D.C. Hambrick, "The Stigmatization and Devaluation of Elites Associated with Corporate Failures: A Process Model," *Academy of Management Rev.*, vol. 33, no. 1, 2008, pp. 231–251.
16. M. Rhee and M.E. Valdez, "Contextual Factors Surrounding Reputation Damage with Potential Implications for Reputation Repair," *Academy of Management Rev.*, vol. 34, no. 1, 2009, pp. 146–168.
17. "Your Ad Here. And Here. And Here," *Businessweek.com*,24 Apr. 2006; www.businessweek.com/magazine/content/06_17 b3981046.htm.
18. E.L. Deci and R.M. Ryan, *Intrinsic Motivation and Self-Determination in Human Behavior*, Plenum Press, 1985.
19. "Online Advertisers Demand Industry Reforms," *Chosun*,15 July 2008.
20. T. Espiner, "Cracking Open the Cybercrime Economy," *ZDNet News*,14 Dec. 2007; http://news.zdnet.com2100-1009_22-180416.html .
21. W.J. Baumol, "Entrepreneurship: Productive, Unproductive, and Destructive," *J. Political Economy*, vol. 98, no. 5, 1990, pp. 893–921.
22. D.C. North Institutions, *Institutional Change and Economic Performance*, Cambridge Univ. Press, 1990.
23. E.A. Kallman and J.P. Grillo, *Ethical Decision Making and Information Technology*, 2nd ed., McGraw Hill, 1996.