Technology Law - Great Google-y Moogley: The Effect and Enforcement of Click Fraud and Online Advertising

Amy Tracy

Follow this and additional works at: https://lawrepository.ualr.edu/lawreview

Part of the Internet Law Commons

Recommended Citation
Amy Tracy, Technology Law - Great Google-y Moogley: The Effect and Enforcement of Click Fraud and Online Advertising, 32 U. ARK. LITTLE ROCK L. REV. 347 (2010). Available at: https://lawrepository.ualr.edu/lawreview/vol32/iss3/5

This Note is brought to you for free and open access by Bowen Law Repository: Scholarship & Archives. It has been accepted for inclusion in University of Arkansas at Little Rock Law Review by an authorized editor of Bowen Law Repository: Scholarship & Archives. For more information, please contact mmserfass@ualr.edu.
TECHNOLOGY LAW—GREAT GOOGLE-Y MOOGLEY: THE EFFECT AND ENFORCEMENT OF CLICK FRAUD AND ONLINE ADVERTISING

I. INTRODUCTION

Online advertising increasingly provides the economic foundation for free press and speech.¹ It benefits consumers and helps small businesses succeed.² Online advertising eclipsed radio advertising in 2007, and by 2011 it is projected to surpass television revenues.³ Online marketing, orders, and delivery are commercial communications between private individuals or commercial entities that take place via electronic networks in electronic commerce (e-commerce).⁴ Click fraud negatively impacts e-commerce by hindering advertisers’ trust, reliance, and profitability on the use and effectiveness of Internet marketing.

Click fraud describes a range of behaviors that generate clicks on Internet advertisements that are not made by potential interested customers, but by people or automated programs for ulterior purposes.⁵ These clicks

¹. An Examination of the Google Doubleclick Merger and the Online Advertising Industry: Hearing Before the Subcomm. on Antitrust, Competition Policy and Consumer Rights of the S. Comm. on the Judiciary, 110th Cong. 5 (2007) (referring to comments made by Bradford L. Smith, Senior Vice President, General Counsel, and Corporate Secretary of Microsoft, Inc., and David Drummond, Senior Vice President of Corporate Development and Chief Legal Officer of Google, Inc.).

². Id.

³. Id. A study by Veronis Suhler, a private equity company focusing on media and communications information, estimates that Internet advertising’s success is due to its targeted, relevant, and measurable approach. Id. Other media forms do not have the same capabilities for searching out consumers. Id.

⁴. COMPUTER LAW: THE LAW AND REGULATION OF INFORMATION TECHNOLOGY 198 (Chris Reed & John Angel eds., Oxford Univ. Press, 6th ed. 2007) [hereinafter COMPUTER LAW].

⁵. See Lambotte v. IAC/Interactive Corp., No. CV 08-04263, 2008 WL 4829882, at *1 n.1 (C.D. Cal. Nov. 4, 2008) (citing plaintiff’s complaint) (defining click fraud as “purposeful clicks on advertisements by someone other than a potential customer”); Brodsky v. Yahoo! Inc., 592 F. Supp. 2d 1192, 1196 (N.D. Cal. 2008) (citing plaintiff’s complaint) (defining click fraud as an “activity under taken for the sole purpose of causing Yahoo! or another search marketing business to log a click which generates a payment due from an advertiser”); NetQuote, Inc. v. Byrd, No. 07-cv-00630-DME-MEH, 2008 WL 2552871, at *13 (D. Colo. June 17, 2008) (citing defendant’s counterclaim) (“[C]lick fraud occurs when ‘a person imitates a legitimate user of a web browser clicking on an ad, for the purpose of generating a charge per click without having actual interest in the target of the ad’s link.’”); Feldman v. Google, Inc., 513 F. Supp. 2d 229, 232 (E.D. Penn. 2007) (“Click fraud occurs when entities or persons, such as competitors or pranksters, without any interest [in the website’s] services, click repeatedly on [an] ad, the result of which drives up [the advertiser’s] cost and discourages . . . advertising. Click fraud may also be referred to as ‘improper clicks’ or ‘trick clicks.’”); In re Miva, Inc., Sec. Litig., 511 F. Supp. 2d 1242, 1249 (M.D. Fla. 2007) (defining click fraud as “the illicit methods of creating Internet traffic . . . advertisers were not forwarded legitimate leads of consumers interested in acquiring their products”); Interactive
increase prices for the advertiser without providing the corresponding commercial benefit that the advertisers expect.\(^6\) Malicious clicks—those made intentionally to defraud a consumer, an advertiser, or the online community—may purposefully generate money for the offending party or, alternatively, may eliminate a competitor’s advertising budget.\(^7\) Google, Inc. (Google) has defined click fraud as the intentional clicking of an online advertisement for a reason “other than to view the underlying content.”\(^8\)

Click fraud is an international problem causing a legal stir in the United States. The largest click fraud settlement took place in 2005 in Texarkana, Arkansas,\(^9\) when Google paid $90 million in a class action attempt to recoup advertisers’ lost dollars.\(^{10}\) The advancement of technology and enhanced online commercial dependency necessitates the creation of strict regulations and legal precedent to protect merchants, consumers, and the online marketplace from fraudulent activity. Civil litigation is insufficient to combat the negative impact that click fraud has on e-commerce. Click fraud should be regulated through defined criminal standards and enforceable methods involving coordinated efforts of the government, private industry, and the public sector.

---

\(^6\) See, e.g., Feldman, 513 F. Supp. 2d at 231–32. The plaintiff was a lawyer who purchased advertising from Google to attract potential clients but instead claimed to be charged for fraudulent clicks. Id. He alleged that although he was originally a member of the class action suit in Arkansas, see Lane’s Gifts discussion infra Part II.C.5, he timely opted out in order to pursue an individual action. Feldman, 513 F. Supp. 2d at 232.

\(^7\) See Payday Advance Plus, Inc. v. Findwhat.com, Inc., 478 F. Supp. 2d 496, 501 (S.D.N.Y. 2007) (citing plaintiff’s complaint). The defendant allegedly hired people to click on certain advertising links to increase revenues. Id.


\(^9\) Miller County, Arkansas was placed on the American Tort Reform Foundation’s watch list for “judicial hellholes” in 2006. AMERICAN TORT REFORM FOUNDATION, JUDICIAL HELLHOLES 22 (2006), available at http://www.atra.org/reports/hellholes/2006/. Miller County saw an increase in major class action lawsuits prior to the enactment of the federal Class Action Fairness Act. Id. It has been considered one of the most “plaintiff-friendly” jurisdictions in the country, which has created a legal environment that encourages companies to settle rather than going to trial. Id. The Google case was just one in a string of major million dollar settlements. Id. The Google case settled for $90 million, Miller County attorneys received $30 million in fees, and the class of plaintiffs only received coupons for future advertising. Id.

In determining the effect of click fraud on e-commerce advertising, this note will identify and explain the concept and origins of click fraud. It will then demonstrate the effect of current click fraud settlements and pending cases as well as the application of Internet and e-commerce law. Next, this note will analyze both civil and criminal litigation tactics, and finally, it will propose guidelines for potential enforcement solutions to regulate click fraud.

II. BACKGROUND

A. The Essence of Internet Advertising

Historically, Internet websites primarily used display-based advertising, such as pop-up ads or banner ads. Google sought to create a more effective, yet unassuming, advertisement geared toward meeting the demands of a niche market. In applying its search principles and building from advertising models used by other search engine companies, Google specialized in search-based advertisement, developing two major advertising forums—AdWords and AdSense.

1. AdWords

Google’s search-based Internet advertising program, AdWords, consists of text-only ads triggered by specific search queries and results patterned after the simplistic design and approach of old-fashioned newspaper advertisements. The ads are distinctly separated from the search results (“organic links”) under a heading entitled “Sponsored Links.”

11. See discussion infra Part II.
12. See discussion infra Part III.A, B.
13. See discussion infra Part III.A, B.
14. See discussion infra Part III.C.
18. VISE & MALSEND, supra note 16, at 86, 89. At the time, GoTo.com was the key Internet advertisement provider, supplying advertisements that appeared with search results on other search engines. Id. at 87. See also Neil Daswani et al., Online Advertising Fraud, in CRIMEWARE: UNDERSTANDING NEW ATTACKS AND DEFENSES § 11.2.2 (Markus Jakobsson &
Advertising in traditional media forms is costly, making it an exclusive club for major companies. Google’s advertising scheme creates equality in the marketplace, allowing local businesses to compete with Fortune 500 companies. Google’s advertisements are only revealed to potential customers in the market for a related specific need or those in a particular geographic location. The AdWords theory depends upon the idea that the searcher would come to the advertiser, much like in a newspaper or advertising on cable television.

AdWords allows advertisers to link keywords to their advertisements so that a search query yields an advertisement for a related product. For instance, a person “googling” “toaster ovens” may find advertisements for Black & Decker (a toaster oven manufacturer), Sears, Target, and Macy’s (retailers that sell toaster ovens). AdWords ads are listed in order of relevance, not price. The highest priced ad does not necessarily appear at the top of the list. Zulfikar Ramzan, eds., 2008). After studying GoTo.com’s methodology, Google’s founders, Sergey Brin and Larry Page, decided they could create their own ads to save money. VISE & MALSEED, supra note 16, at 87–88. The key to their advertising success, however, would be making it clear that the ads would not bias the search results. Id. at 88–89.


26. VISE & MALSEED, supra note 16, at 90. PageRank is a process used by Google for tracking a website’s popularity by counting the number of links that direct users to a site. Id. at 37. Google uses PageRank in web searches to return prioritized results based on relevance.
top of the page. Google's advertising system allows its users to rank the ads, making the most clicked ads the most relevant. The most relevant ads appear at the top of the page. Search-based advertising accounted for approximately $5.1 billion in 2005, 41% of total Internet advertising revenue. In 2008, interactive advertising amounted to $300 billion in economic activity. Since the creation of the AdWords program in 2002, Google experienced a 409% revenue growth rate in 2002 and a 234% revenue growth rate in 2003. Both Google's total revenue and total advertising revenue continue to increase through 2009.

2. AdSense

As AdWords became more successful, Google was able to create an affiliate program—AdSense—which enabled other web sites, such as AOL, EarthLink, HowStuffWorks, and Blogger, to buy Google's ads to place on their websites. There are two ways for website publishers to participate in

Id. at 37–39. Unlike other search engines that simply match words in queries to words found on a web page, Google uses PageRank to put search results in a logical order for users. Id. The same theory is applied to Google's advertising scheme. Id. Google's co-founders were originally convinced that advertising on search engines led to biased results and an impure PageRank—they recognized that advertising income often provides an incentive to provide poor quality search results and an inclination to simply direct users to advertising partners. Id. Advertising is also a means to fund Google's goal of organizing the world's information and making it universally accessible and useful in an impartial manner. Id. See also SERGEY BRIN & LAWRENCE PAGE, THE ANATOMY OF A LARGE-SCALE HYPERTEXTUAL WEB SEARCH ENGINE 8 app.a (1998), available at http://ilpubs.stanford.edu:8090/361/1/1998-8.pdf (report written by Brin and Page while graduate students at Stanford detailing their new internet program, Google).

27. VISE & MALSEED, supra note 16, at 90.
28. Id.
29. Id.
34. Google AdWords Help: What is Google AdWords, http://adwords.google.com/support/bin/answer.py?hl=en&answer=6084 (last visited Mar. 8,
the AdSense program: *AdSense for search* and *AdSense for content*.\(^3\)5 *AdSense for search* allows Google to place its ads on individual publishers' websites.\(^3\)6 When a user inputs keyword-based searches on a publisher's site, the search results pages will contain Google ads that fit the theme of the publisher's website.\(^3\)7

*AdSense for content* is a system that automatically delivers targeted ads to a publisher's web page.\(^3\)8 The ads are based on the content of the visited pages and the geographical location of the user, determined by an Internet Protocol Address (IP address).\(^3\)9 These ads are usually preceded by the heading "Ads by Google."\(^4\)0 Google displays ads on a publisher's website that are relevant to the user, while also providing ads that will trigger clicks to maximize revenues.\(^4\)1 Ironically—for a company that was initially opposed to advertising—ninety-nine percent of Google's current revenue is derived from AdWords and AdSense.\(^4\)2

B. Payment Methods for Online Advertising

Google's AdWords program uses a payment method similar to most other Internet advertising schemes. AdWords is based on the Pay-Per-Click (PPC) method (sometimes referred to the Cost-Per-Click (CPC) method), which allows an advertiser to pay only when a visitor clicks on its ad.\(^4\)3 In

---

35. Tuzhilin, supra note 22, at § 7.2.
36. Id. See also Daswani et al., supra note 18, at § 11.2.2.
37. Tuzhilin, supra note 22, at § 7.2.
38. Id.
39. Id. An Internet Protocol address (IP address) is "the ten-digit identification tag used by computers to locate specific websites." BLACK'S LAW DICTIONARY 836 (8th ed. 2004).
40. Tuzhilin, supra note 22, at § 7.2.
41. Id. at 11.
42. 2007 Annual Report, supra note 8, at 20. Click fraud uses AdWords to corrupt advertising revenues through false clicking. See Feldman v. Google, Inc., 513 F. Supp. 2d 229, 232 (E.D. Penn. 2007). AdSense is essentially infiltrated in the same manner, except individual publishers initiate the false clicks to increase revenues garnered from advertising on their personal websites using Google advertisements. See generally discussion supra Part II.A.1, 2. See also Tuzhilin, supra note 22, at § 12.
43. Tuzhilin, supra note 22, at § 8. Other payment methods include the Cost-Per-Mille or Cost-Per-Impression (CPM) and the Cost-Per-Action (CPA) models. Id. at § 7. The CPM method allows an advertiser to pay per one thousand impressions of the ad. Id. An impression occurs each time a Google search result is displayed for an item. Daswani, et al., supra note 18, at § 11.2.1. In the CPA method, an advertiser pays when a certain conversion action takes place, such as a product being purchased online, an advertised item is placed into a shopping cart, or an online form is filled out. Tuzhilin, supra note 22, at § 7. From the advertisers' point of view, this is the most effective type of advertisement payment plan because it ensures that the advertisement actually targeted a customer who reacted positively to the advertisement. Id.
using a PPC method, Google sets its per-click price using an auction system, which collects advertising payments contingent upon the validation of clicks.\textsuperscript{44} Each advertiser bids according to how much it is willing to pay per click for a particular keyword.\textsuperscript{45} Other advertisers vie for the same keyword, causing the price per click to increase.\textsuperscript{46} An advertisement's page position is based on the price a company is willing to pay in the auction and the ad's popularity, or how frequently it is clicked.\textsuperscript{47}

C. The Challenge of Click Fraud

Google's PPC advertising scheme has become susceptible to corruption through click fraud.\textsuperscript{48} Click fraud—clicks made by people or automated programs for ulterior purposes—drives up prices for the advertiser without providing the corresponding commercial benefit that the advertisers expect.\textsuperscript{49}

1. Types of Click Fraud

There are typically three different types of clicks: valid, invalid, and malicious.\textsuperscript{50} A click is typically categorized based on the intended action and purpose of the clicker.\textsuperscript{51}

Valid clicks occur when a consumer in the online marketplace clicks on a sponsored link or advertisement with the intent to gain additional information or to purchase goods.\textsuperscript{52} Valid clicks are the basis for intended online advertising profit.\textsuperscript{53}

Invalid clicks consist of accidental or unintended double clicks, web browser errors, or a consumer clicking on a link and using the "back" button to retrieve something previously viewed.\textsuperscript{54} Click fraud does not include

\begin{itemize}
\item \textsuperscript{44} Google AdSense Terms and Conditions, https://www.google.com/adsense/localized-terms (last visited Mar. 8, 2009). The auction system was originally created by Overture, an Internet advertising company who supplied Yahoo! with its ads. \textit{Vise \& Malseed, supra note 16, at 115–16.}
\item \textsuperscript{45} \textit{Vise \& Malseed, supra note 16, at 115–16.} Google's only price-setting guideline is that the minimum bid must be five cents. \textit{Id. at 117.}
\item \textsuperscript{46} \textit{Id. at 115–16.}
\item \textsuperscript{47} \textit{Id. at 117.}
\item \textsuperscript{48} Daswani et al., \textit{supra note 18, at § 11.2.2.}
\item \textsuperscript{49} See \textit{supra} notes 5–6.
\item \textsuperscript{50} See \textit{Tuzhilin, supra note 22, at §§ 16–18.} \textit{See also} Daswani et al., \textit{supra note 18, at § 11.3.2.}
\item \textsuperscript{51} See \textit{Tuzhilin, supra note 22, at §§ 16–17.} \textit{See also} Daswani et al., \textit{supra note 18, at § 11.3.2.}
\item \textsuperscript{52} See \textit{Tuzhilin, supra note 22, at § 17.}
\item \textsuperscript{53} See \textit{id.}
\item \textsuperscript{54} \textit{Id. at §§ 16–17.}
\end{itemize}
invalid clicks, although they are tracked because they may skew click fraud statistical data.\textsuperscript{55}

The third type of click is the foundation of click fraud. Malicious clicks are made intentionally to defraud a consumer, an advertiser, or the online community with the purpose of generating money for an individual or company or for eliminating a competitor's advertising budget by falsely using paid clicks.\textsuperscript{56} Google has defined click fraud as the intentional clicking of an online advertisement for a reason "other than to view the underlying content."\textsuperscript{57}

2. \textit{The Adverse Effects of Click Fraud and How Click Fraud is Perpetrated}

Fraudulent clicking activity eliminates a company's advertising budget, causing a search engine to eliminate an ad once the PPC limit is reached.\textsuperscript{58} As a result, a competitor is able to purchase the previously eliminated advertising keyword and ad position for a lower price.\textsuperscript{59}

Malicious clicks originate from three basic sources: business competitors, individual publishers, and clickbots.\textsuperscript{60} Business competitors are the most common click fraud perpetrators. For example, Company \#1 commits X dollars per month to Google for advertising on a PPC basis. Every time someone clicks on the company's ad, money is deducted from its AdWords account. Eventually, the company will reach its maximum amount of paid clicks, and its ad will be eliminated until more PPC advertising is purchased.

\begin{footnotes}
\textsuperscript{55} Id.
\textsuperscript{56} See id. at § 17. See also Daswani et al., \textit{supra} note 18, at § 11.3.2.
\textsuperscript{57} 2007 Annual Report, \textit{supra} note 8, at 25.
\textsuperscript{58} Daswani et al., \textit{supra} note 18, at § 11.3.2.; Feldman v. Google, Inc., 513 F. Supp. 2d 229, 232 (E.D. Penn. 2007) ("The price per keyword is determined by a bidding process, wherein the highest bidder for a keyword would have its ad placed at the top of the list of results from a Google.com search by an internet user.").
\textsuperscript{59} See Tuzhilin, \textit{supra} note 22, at §§ 10, 18.
\textsuperscript{60} Id. at §§ 17–18; Daswani et al., \textit{supra} note 18, at § 11.4. The five major classes of invalid clicks that affect advertising profits include: 1) Bad Spiders: clicks inadvertently made by a webcrawler while gathering Internet pages for search engines; 2) Speed Demons: clicks arising from Internet service providers or wireless devices because the system works too slow and an impatient user clicks multiple times; 3) Commission Collectors: clicks made by individuals to gain a profit; 4) Sore Losers: clicks that are made by an individual or a bot to cause intentional costs to a competitor; and 5) Badware: clicks arising from an adware or pop up ad program that essentially tricks a user to click into unwanted territory. SEAN HARVEY, \textit{INVALID CLICKS AND ONLINE ADVERTISING}, DOUBLE CLICK WHITE PAPER 1 (April 2007), available at http://www.doubleclick.com/insight/pdfs/dc_invalid_clicks_0704.pdf. See \textit{supra} note 15 (information on Doubleclick, Inc.); see infra note 66 (detailing bots).
\end{footnotes}
Archivial Company #2 wants to undermine Company #1’s advertising revenue in an attempt to become number one in the industry. Company #2 hires an “employee” to click Company #1’s sponsored link on Google all day, every day. Eventually, Company #1’s ad disappears because it has run out of paid clicks. Company #2 prevails and Company #1 loses its advertising, customers, and revenue without having a single valid customer visit its website.

Click fraud also affects AdSense. Individual publishers make a percentage of profit per-click through AdSense. To increase revenues, dishonest publishers may click on the advertisements on their own web pages to increase their profits. By clicking on the ads, publishers increase the popularity of their site, which in turn increases the PPC, and thus increases revenues for the publisher.

In some situations, hackers have compromised computers and installed programs (“clickbots” or “bots”) to automatically log false clicks on hundreds of thousands of Google advertisements each minute. This method of click fraud eliminates PPC budgets instantaneously.

3. Google’s Attempt at Combating Click Fraud

Although click fraud is not per se illegal, its deceptive nature and dishonest accrual of profits presents the illusion of a criminal offense. To protect its customers against click fraud, Google has imposed three major de-
fenses: detection and filtering techniques, advanced monitoring techniques, and the Google Click Quality Team.\footnote{67}{Google AdWords Help: How Does Google Detect Invalid Clicks?, http://adwords.google.com/support/bin/answer.py?hl=en&answer=6114 (last visited Mar. 8, 2009) [hereinafter AdWords Help]. See generally Tuzhilin, supra note 22, at §§ 21–44; Daswani, et al., supra note 18, at § 11.5.2.}

a. Detection and filtering

Google's detection and filtering techniques examine each click on an AdWords ad for data points, such as the IP address,\footnote{68}{See supra note 39 (defining IP address).} the time of the click, any duplicate clicks, and various other click patterns.\footnote{69}{AdWords Help, supra note 67. See also Tuzhilin, supra note 22, at §§ 21–44; Daswani, et al., supra note 18, at § 11.5.2.} The system then analyzes the data points and attempts to isolate and filter potentially invalid clicks before they count as a PPC action.\footnote{70}{AdWords Help, supra note 67.}

b. Advanced monitoring techniques

Additionally, Google works to detect invalid clicks so that they may be identified before an advertiser is billed.\footnote{71}{Kevin Newcomb, Google Offers More Click Fraud Data, SEARCH ENGINE WATCH, Mar. 1, 2007, http://searchenginewatch.com/showPage.html?page=3625137. Search Engine Watch is a leading website for timely news and information regarding search engine action. Vise & Malseed, supra note 16, at 83. Search Engine Watch originated at approximately the same time as Google, and has followed the search engine extensively. Id.} Google uses real-time filtering and offline analysis to meet these objectives.\footnote{72}{See generally Tuzhilin, supra note 22, at §§ 23, 35; Daswani, et al., supra note 18, at § 11.5.2.} Catching clicks in real-time allows Google to filter the clicks so that it appears to advertisers as though they never occurred.\footnote{73}{Kevin Newcomb, Google Offers More Click Fraud Data, SEARCH ENGINE WATCH, Mar. 1, 2007, http://searchenginewatch.com/showPage.html?page=3625137. Search Engine Watch is a leading website for timely news and information regarding search engine action. Vise & Malseed, supra note 16, at 83. Search Engine Watch originated at approximately the same time as Google, and has followed the search engine extensively. Id.} The real-time net filters a specific profile of invalid behavior, such as excessively repetitive clicks or clicks and impressions from known sources of invalid activity.\footnote{74}{See generally Tuzhilin, supra note 22, at §§ 23, 35; Daswani, et al., supra note 18, at § 11.5.2.} Not all the clicks that are removed can be classified as fraudulent clicks, but they may be deemed questionable—the clicker may have a malicious or impure intent to profit from the click.\footnote{75}{Shuman Ghosemajumder, Business Product Manager for Trust and Safety of Google, Inc., stated that "when we proactively remove these clicks, we forego a significant amount of revenue. We’re providing hundreds of millions of dollars in proactive protection." Newcomb, supra note 71. Every one percent of clicks removed proactively would equate to $100 million in lost annual revenue for Google. Id.}
c. Google’s Click Quality Team

Offline analysis—click inspection after a click is recorded—is another proactive detection technique executed by Google’s Click Quality Team ("the Team").

Clicks detected during offline analysis are not billed to the advertiser, but they still show up on advertisers’ monthly click revenue data.

The Click Quality Team was created in 2004 as a self-regulating device. The Team’s continuing goal is to make invalid click activity difficult and unrewarding for unethical users. The Team continues to implement and apply strategies designed to help advertisers to report suspected click fraud and block Google from serving ads to specific IP addresses, as well as creating and using new anti-click fraud technology. Additionally, Google refunds its advertisers for invalid clicks that are initially undetected by the company.

In 2007, Google estimated its click fraud percentage to be less than ten percent of all clicks.

Despite Google’s attempts, critics argue that Google has not confronted click fraud head-on because allowing click fraud actually enables Google to profit in the short-term. For every ad falsely clicked, Google gets paid. Google denies the accusations and claims that it is improving its anti-click fraud policies but cannot be excessively transparent regarding its methods because “fraudsters” will find a way to beat the current technology.

---

76. Id.
77. Id.
79. AdWords Help, supra note 67.
80. See Tuzhilin, supra note 22, at § 21.
82. Daswani et al., supra note 18, at § 11.5.3. Google’s click fraud statistics may vary from third-party statistics because they define invalid clicks differently, leading to inconsistent results. Id. at § 11.6.2.
84. “Fraudster” is a term of art used by Google, technology experts, the news media, and technology experts to describe the individuals or bots engaged in click fraud. See generally Daswani et al., supra note 18, at § 11 (discussing fraudsters throughout).
85. Id. at § 11.5.1.
4. Independent click fraud consultants

Search engines, publishers, and clickers all unduly profit from click fraud. Recognizing the need for third-party, unbiased click fraud data, independent consulting firms are beginning to materialize. Click Facts, a San Francisco-based consultant, works to protect advertising network providers and online advertising buyers from malicious web attacks in an attempt to make digital advertising safer.\(^8\) Click Forensics, an Austin-based click fraud consultant, tracks and monitors data gathered from its Click Fraud Index, a network of more than 4,000 online advertisers and agencies.\(^8\) The Click Fraud Network provides statistical PPC data collected from advertising campaigns, large and small, across all the leading search engines.\(^8\) In the fourth quarter of 2008, Click Forensics reported that the overall industry click fraud average rate was 17.1%.\(^9\) Click Forensics also reported that the methods used to commit click fraud, such as an increase in clickbot Web traffic, have become increasingly more sophisticated and difficult to detect.\(^9\)

5. Alternative click fraud remedies

In addition to self-regulatory efforts and private consulting, various civil legal theories have been used to address the problem of click fraud.\(^9\) In July 2006, Google reached a $90 million settlement with a class of unsatisfied AdWords advertising customers in Texarkana, Arkansas.\(^9\) The class in *Lane's Gifts v. Yahoo!, Inc. and Google Inc.* alleged breach of contract

---

\(^9\) Id.
\(^9\) Id.
\(^9\) Id.
\(^9\) Id.


\(^9\) Final Order and Judgment Approving Settlement, Certifying Class for Settlement Purposes, Awarding Class Counsel Attorneys' Fees and Dismissing Action with Prejudice at 7, *Lane's Gifts*, No. CV-2005-52-1. The class action was initially filed in the Miller County Circuit Court before being filed in federal court by a local Arkansas business, Lane's Gifts and Collectibles. Plaintiffs' Second Amended Complaint, *supra* note 91. The action targeted big name search engines like Yahoo!, Google, and America Online for excessive advertising charges based on fraudulent clicks. *Id.* Because the interstate class action was of national importance, it was later filed in federal court to secure a fairer outcome pursuant to the Class Action Fairness Act of 2005. *Id.* See also 28 U.S.C. §§ 1332(d), 1453, 1711–14 (2000).
under the terms of the pay per click agreement, unjust enrichment, and civil conspiracy.  

While Lane's Gifts was being decided, Advanced Internet Technologies, Inc. (AIT), v. Google, Inc. was granted a stay request for their action alleging breach of contract, negligence, unjust enrichment, and unfair business practices relating to click fraud. The Lane's Gifts parties settled; therefore, no precedent was created. The AIT case was dismissed as a result.

In June 2009, Microsoft filed a click fraud action against three Canadian residents in the federal District Court for the Western District of Washington. Microsoft is the first corporation to file a click fraud suit, creating a new scenario where the company, not a consumer, is the "victim." Microsoft alleged a massive click fraud scheme on an online advertising network operated by the company, citing breach of contract; breach of implied covenant of good faith and fair dealing; tortious interference with a business relationship; fraudulent concealment; fraudulent misrepresentation; civil conspiracy; and violations of the federal Computer Fraud and Abuse Act, the Washington Computer Spyware Act, and the Washington Consumer Protection Act. Microsoft realized false clicks were being logged under the guise of multiple IP addresses for specific searches target-
ing automobile insurance and World of Warcraft, an online role playing game. If the Microsoft case goes to trial, it will create an important precedent and foundation for the future regulation of electronic crime. Microsoft seeks injunctive relief, $750,000 in compensatory damages, and other fees and damages.

There have also been governmental attempts at click fraud enforcement. The Federal Bureau of Investigation has launched investigations in coordination with a specialized unit of Northern District of California United States Attorney's Office—the Computer Hacking and Intellectual Property Unit (CHIP). These agencies have attempted to prosecute domestic click fraud under civil causes of action.

 Probably the most creative response to the click fraud problem is bypassing search engines, litigation, consultants, and the government and alerting a credit card company of a fraudulent charge based on a payment for advertising. This “solution” leaves it to the credit card company to sort out the overcharge; however, it does not resolve the issue.

103. Complaint for Injunctive Relief and Damages, supra note 98 at ¶ 27. Defendants allegedly registered for four Microsoft advertising accounts. Id. Microsoft credited automobile insurance and World of Warcraft advertisers $1.5 million for losses sustained from click fraud, and Lam, as an "advertiser" received his share after lodging a complaint. Id. at ¶ 35. Although Lam may have requested and received a credit in an attempt to look innocent, Microsoft linked Lam to the click fraud scheme by tracing the false click IP addresses to computers or servers operated or registered by Eric Lam. Id. at ¶ 33. Lam used the computers to sell World of Warcraft gold. Id. at ¶ 33.

104. Complaint for Injunctive Relief and Damages, supra note 98 at ¶¶ 89-96.

105. Press Release, Department of Justice, supra note 91. A California man was indicted by a federal grand jury for using a source code obtained by his employer to develop a click-bot to fraudulently generate points from an Internet click fraud scheme by clicking on advertisements, completing consumer surveys, and making online purchases. Id. He later used the points to buy products from Internet retailers. Id. The man was charged with conspiracy, mail fraud, and wire fraud. Id.


III. PROPOSAL

Click fraud may be combated through several different approaches—civil causes of action, criminal statutes, search engine self-regulation efforts, or third party involvement. Click fraud must be resolved in a court of law rather than through the course of business dealings. Treating click fraud as a civil wrong allows advertisers to recoup false advertising charges and receive restitution, making amends but not correcting the problem. With the advent of the Internet as a primary commerce tool, restitution may not be enough. Electronic commerce must occur in a reliable and trustworthy setting; click fraud disrupts this goal. Applying criminal penalties to click fraud would punish such behavior and deter it in the future. Involving search engines and third party efforts would provide enforcement and technical expertise that otherwise may not be available.

A. The Legal Challenges of Click Fraud

The concept of fraudulent clicks is difficult to understand, difficult to track, and difficult to classify under law. Furthermore, it is difficult for plaintiffs to demonstrate how and why clicks are fraudulent and that actual legal injury or economic harm occurred. This may be the reason general civil causes of action are used to circumvent the click fraud issue—recognizing a breach of contract may be easier than introducing the concept of click fraud. Proving a fraudulent click is difficult because there is not one, true definition—there is no accepted industry standard constituting a fraudulent click.

Determining who should be responsible for the alleged fraud is another major issue. While search engines are the easiest party to target, click fraud may be perpetrated by a number of individuals or parties. A search engine forges a contract with an advertiser and sets the terms of a PPC arrange-

110. Telephone interview with Michael Caruso, supra note 109.
111. Daswani et al., supra note 18, at § 11.6.2. Third party consultants may find a different percentage of fraudulent clicks than a search engine in a given period because of the method and definition used in determining valid clicks. Id. Auditing companies are not privy to information regarding what clicks search engines actually charge for, so they may have to make an educated guess at what may or may not be valid. Id.
ment. The search engine, however, is not the party logging the fraudulent click. The actual fraudulent click is made by a clicker or a bot; unfortunately, these parties are difficult to identify and track down because of the anonymity of the Internet. Until the issue of click fraud was first identified, search engines had no need to track clicks, measure metrics or conversion rates, worry about abuse of the system, or wonder if they were unintentionally overcharging advertising fees.

Widespread regulation is needed because click fraud is an international issue and the current methods of circumventing click fraud are too broad. Standard and predictable click-fraud provisions are necessary for deterrence and remedy. It is important to evaluate the legal framework in which click fraud regulation may occur. The United States court system has not set a precedent for click fraud, nor does any law specifically mention its existence. Search engines have become more self-regulated, but this may not be enough. Click fraud must be combated to protect consumers, maintain the effectiveness of online advertising, and encourage future e-commerce development.

B. Analysis of Click Fraud Combat Approaches: Civil Theories

Eric Goldman, noted technology law expert, questioned the attachment of the civil conspiracy cause of action in the Lane’s Gifts case. This is a common cause of action in Arkansas in contract cases. In Faulkner v. Arkansas Children’s Hospital, civil conspiracy was defined as “two or more persons combined to accomplished a purpose that is unlawful or oppressive or to accomplish some purpose, not in itself unlawful, oppressive, or im-

113. See discussion supra Part II.B.
114. See discussion supra Part II.C.2.
115. See supra note 60.
116. See discussion supra Part II.C.3.
117. See Daswani et al., supra note 18, at § 11.4.1. Instances of false clickers and clickbots have been identified in South Korea, Egypt, the Ukraine, Bulgaria, the Czech Republic, Mongolia, Vietnam, and Honduras. Brian Grow & Ben Elgin with Moira Herbst, Click Fraud: The Dark Side of Advertising, BUSINESS WEEK, Oct. 2, 2006, at 46, available at http://www.businessweek.com/magazine/content/06_40/b4003001.htm; Brian Grow, Doing Business with a Controversial Partner, BUSINESS WEEK, Oct. 2, 2006, at 57, available at http://www.businessweek.com/magazine/content/06_40/b4003012.htm.
118. See discussion supra Part III.C.1.
119. See, e.g., NetQuote, Inc. v. Byrd, No. 07-cv-00630-DME-MEH, 2008 WL 2552871, at *14 (D. Colo. June 17, 2008) (holding that “there is no indication that Georgia has adopted the tort of ‘click fraud’”).
120. AdWords Help, supra note 67. See also discussion supra Part II.C.3.
121. See GOLDMAN, CLICK FRAUD CONFERENCE, supra note 108. See also Plaintiffs’ Second Amended Complaint, supra note 91.
moral, but by unlawful, oppressive, or immoral means, to the injury of another.” Civil conspiracy is not actionable in and of itself, but it allows recovery of damages caused by acts committed pursuant to the conspiracy. Goldman compares civil conspiracy to antitrust and competition law, stating that taking an antitrust approach in opposing click fraud may raise the stakes for search engines. Antitrust infers a conspiracy in a market relationship. Combating click fraud through the Sherman Antitrust Act would ensure click fraud’s illegality and apply stiff penalties.

Many of the civil claims against advertising overcharges have focused on fraudulent behavior. Common law fraud, however, is a generic term, and direct evidence of fraud may be difficult to obtain. The only way to demonstrate that fraud has occurred is by keeping rationally and consistently developed, documented, and implemented records of alleged fraudulent activity.

Generally, contract law and business dealings allow for restitution, but do not deter incidents of future misconduct. If the goal of legal action for click fraud is to get advertisers’ money back, civil means are sufficient. If the goal is to prevent, deter, and punish those responsible for click fraud, however, criminal penalties must be applied.

C. Analysis of Click Fraud Combat Approaches: Criminal Theories

As Internet technology evolves in the absence of enforcement and regulation, click fraud will become more prevalent. There are currently state and federal criminal statutes relating to theft and fraud, but these statutes

123. Id.
124. See Goldman, Click Fraud Conference, supra note 108.
125. Id.
126. The Sherman Antitrust Act states, in pertinent part:

Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal. Every person who shall make any contract or engage in any combination or conspiracy hereby declared to be illegal shall be deemed guilty of a felony, and, on conviction thereof, shall be punished by fine not exceeding $100,000,000 if a corporation, or, if any other person, $1,000,000, or by imprisonment not exceeding 10 years, or by both said punishments, in the discretion of the court.

128. Id. at § 11.02.
129. Telephone interview with Michael Caruso, supra note 109.
may not be specific enough to target click fraudsters. Nevertheless, they may still be more effective than civil claims in combating click fraud.

1. **State Criminal Theft and Fraud Statutes**

Sections 5-41-201 through -206 of the Arkansas Code detail criminal penalties for computer crimes. Furthermore, sections 5-36-104, -106, and 5-37-101 provide for instances of general theft and fraud. Other states have similar statutes. While click fraud may be interpreted to fall within the language of these state statutes, there is a question of who should prosecute the matter—the state or the federal government. Although States may be able to spend more time on the problem, the nature of the crime appears to require federal involvement, which has typically been implemented in other internet crimes.

2. **The Federal Computer Fraud and Abuse Act**

The Computer Fraud and Abuse Act, amended as recently as 2008, concerns computer fraud and related activity and applies punishment for unauthorized computer hacking. The statute, which does not specifically address click fraud, states that “[w]hoever intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss” may be punished by varying degrees of fines or imprisonment. A “protected computer” is defined as “a computer which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the...
United States." It appears that this provision could be interpreted to include fraudulent clicks made by clickbots, which would enable criminal penalties to be applied to fraudsters.

In *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*, the court held that the Computer Fraud and Abuse Act provision forbidding obtaining information from a protected computer involved in interstate and foreign commerce applied to private actions because there was alleged fraud or loss. This holding supports application of federal law, even though the click fraud dispute may be between private parties.

### 3. The Wire Fraud Act

The Wire Fraud Act has also been used to punish fraud on the Internet. The Act states:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

In *United States v. Blanchett*, the defendants fraudulently received $34,000 by selling nonexistent computer equipment on eBay, an Internet auction site. The penalty for the defendants’ acts was enhanced because they attempted to defraud more than one victim using mass marketing.

Similarly in *United States v. Pirello*, the court held that an enhanced penalty for mass marketing was appropriate when a defendant defrauded consumers by placing a classified advertisement for computers on an Internet bulletin board.

---

137. *Id.* § 1030(e)(2)(B).
138. This has not been confirmed by legislative history or case law, however, because the specific crime of click fraud is nearly nonexistent in the current legal provisions or decisions.
140. *Id.*
142. *Id.*
143. 41 F. App’x 181, 2002 WL 511745 (10th Cir. 2002).
144. *Id.*
145. 255 F.3d 728 (9th Cir. 2001). The *Pirello* dissent questions the interpretation of the phrases “mass-marketing” and “solicitation” as they are used by the Federal Sentencing Guidelines in determining an appropriate punishment for wire fraud. *Id.* at 733 (Benzon, J., dissenting). Circuit Judge Benzon suggests that solicitation is a one-on-one act which cannot
These examples of wire fraud used advertising to defraud consumers of money, which is also the primary goal of click fraud—although it obtains the money through more advanced technological means. If criminal penalties can be applied to selling computer parts that do not exist, they should also be applied to fraudulent clicks which falsely charge advertisers.

4. The Unlawful Gambling Enforcement Act

Additional Internet regulation can also be found in The Unlawful Internet Gambling Enforcement Act,\textsuperscript{146} which bars businesses from knowingly accepting payments in connection with unlawful Internet gambling and prohibits gambling websites from turning any computer into a casino.\textsuperscript{147} The Act uses agencies and commissions to enforce Internet crime and promote public welfare—an approach that may be effective in combating click fraud.\textsuperscript{148}

D. Miscellaneous Click Fraud Combat Approaches

Individual Internet Service Providers (ISPs) may take a stand against click fraud. An ISP acted as an independent regulator by denying Internet access to a company who provided a safe haven for Internet spam groups and for its "misuse" of the Internet.\textsuperscript{149} While this approach may not deter click fraud extensively, it can act as a delay tactic until state or federal sanctions are applied or another solution arises.

E. Guidelines for a Solution

Although existing civil and criminal approaches may be used to combat click fraud, Internet technology is rapidly changing. A click fraud solution must use and execute existing standards of law in a flexible and unprecedented manner, expanding the scope of enforcement to include not only the government, but search engines, private industry, and the public sector as well.

\textsuperscript{146} Codified at 31 U.S.C. §§ 5361–5367 (West 2009).
\textsuperscript{147} 12 C.F.R. §§ 233.1–233.7 (2008). The Act was officially instituted by the United States Treasury Department and the Federal Reserve on November 12, 2008. \textit{Id}. Internet gambling companies have until December 1, 2009, to comply with the rule. \textit{Id}.
\textsuperscript{148} \textit{Id}.
1. Regulation of Electronic Markets

The principles of electronic market regulation must be considered in implementing click fraud regulation. The goal of e-commerce regulation is to promote a fair market, which does not occur by overcharging for advertising based on fraudulent clicks or enabling clicks to generate income for malicious causes. Several factors to consider in applying regulation include: 1) whether a market is open; 2) whether regulation can be abused to mislead or take advantage of anyone; 3) whether regulation can handle trading reliability; and 4) whether regulators have jurisdiction of the market.

Regulation must be facilitated on a global basis and in a manner that does not hinder technological advancement. The Internet market changes daily. When the market changes, the application of the law must either be reassessed or be flexible enough to bridge the change. Electronic markets are characterized by faster dissemination of information, greater trading volume, diversity, and geographic dispersal. Any attempt to regulate click fraud must take ever-changing technological characteristics into account.

2. Enhanced Search Engine Self-Regulation Efforts

Stephen Malouf, plaintiffs lead counsel for the Lane’s Gifts case, stated that search engines seem to do a good job with self regulation. Malouf questioned the necessity for outside regulation, stating that legislation would most likely use “reasonable efforts” as a quantitative term. Attempting to prove reasonable efforts in court would be a “litigation nightmare” because it becomes a factual question of clicker’s intent.

Enhanced self-regulation efforts, however, may help in prosecuting click fraud. The problem with litigation is that the intent to commit click fraud is difficult to understand and prove. A search engine, however, may...
be able to collect click data which could be used to help determine clicker intent.\footnote{161} Google's Click Quality Team collects information about invalid clicks and analyzes click activity.\footnote{162} Mandated search engine protocol for obtaining and publishing data would help avail information for litigation—transparency would increase and the burden of proving intent would decrease.\footnote{163}

3. Third Party Involvement: Private Industry and Public Sector Efforts

Third-party involvement may come in the form of public sector or private entity involvement in educational opportunities, consulting, auditing, and general awareness efforts. Private entity efforts regarding click fraud currently exist as those in the Internet business recognize the challenges of the electronic market.\footnote{164} The Internet Advertising Bureau (IAB), which has been working toward click fraud management for two years,\footnote{165} was founded in 1996 with the goal of growing the interactive advertising marketplace; educating marketers, agencies, media companies, and the wider business community about the value of interactive advertising; evaluating and recommending standards and practices; and fielding research on interactive advertising.\footnote{166} An organization such as IAB\footnote{167} may aid in the enforcement of click fraud or serve as an advisory committee for regulatory efforts.\footnote{168} On the other hand, a regulatory committee composed solely of those in the marketplace, including possible offenders, may actually hinder progress in combating click fraud.

The public sector, in contrast, may not know the obstacles that click fraud presents. The public sector, including advertisers using PPC programs, has typically accepted the ramifications attached to false clicks.\footnote{169} As the economy becomes weaker, however, every dollar will count and advertisers will be more apt to question Internet advertising billing practic-

\footnote{161} Id.
\footnote{162} See discussion supra Part II.C.3.c. See also Newcomb, supra note 71.
\footnote{163} Transparency may include publishing false click data, search engine auditing, click quality control reporting, or any other method of making click fraud information and combat attempts public to promote fair dealing. Telephone interview with Michael Caruso, supra note 109.
\footnote{164} Id.
\footnote{165} Id.
\footnote{166} IAB.net, About the IAB, http://www.iab.net/about_the_iab (last visited Jan. 24, 2009).
\footnote{167} IAB is comprised of more than 375 leading media and technology companies responsible for selling eighty-six percent of online advertising in the United States. Id.
\footnote{168} Id.
\footnote{169} Telephone interview with Michael Caruso, supra note 109.
es. This, in turn, will most likely garner media attention, thereby informing the general public about the dangers of click fraud.

Consumer awareness of click fraud poses additional legal considerations. Buying Internet advertising is a voluntary activity, and buying it knowing that click fraud is a possibility could be construed as a waiver if litigation were to ensue. As e-commerce continues to evolve, however, there might not truly be a choice to forego online advertising opportunities, creating a defense to a waiver agreement.

a. Education

Education aids current and future online advertisers in understanding the risk of click fraud. As a result of the *Lane's Gifts* settlement and the *AIT* case, certain private companies and individuals have rallied to educate the masses. For instance, Lostclicks.com is a website dedicated to informing consumers about the hazards of click fraud and recruiting members for the *Lane's Gifts* class action suit.

Based on the educational premise, click fraud consulting has gained credibility and popularity. Third-party groups like Click Facts and Click Forensics conduct research to determine the effects of click fraud. Consultants act as a search engine industry watchdog in ensuring that search engines fulfill their self-regulatory actions. These consulting firms also help legal counsel understand click fraud and its effects when preparing for trial or settlement.

The future of consulting may evolve into a third party clearing house model that will help regulate the click fraud industry by auditing click fraud figures and taking the advertising details out of the search engine’s hands. For instance, Google will still run its AdWords program, but a third party

---

170. Id.
171. Id.
172. See Goldman, Click Fraud Conference, supra note 108.
173. Id.
176. See Clickfacts, supra note 175; Click Forensics, supra note 175.
177. Jeff Martin, Click Fraud Case to Stay in Arkansas, Vericlix, http://www.vericlix.com/2005_09_11_ppcfraudwatch_archive.html (referencing Stephen Malouf’s, (the plaintiffs' counsel in the *Lane's Gifts* case) belief that a third-party system is the future of click fraud regulation in which PPC networks and advertisers would grant third parties access to their data.)
clearing house would distribute the ads, collect the money for Google, and monitor click fraud attempts. This model eliminates search engines' temptation to allow click fraud.

b. Principles of Government Involvement

President Clinton and Vice President Gore created a Framework for Global Electronic Commerce in 1997, which detailed five basic principles in applying government regulation. The principles include recognition that: 1) the private sector should lead; 2) governments should avoid undue restrictions on electronic commerce; 3) where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce; 4) governments should recognize the unique qualities of the Internet; and 5) electronic commerce over the Internet should be facilitated on a global basis.

President Obama released a Cyberspace Policy Review in 2009 following a sixty-day comprehensive review of the existing state of cyber security in the United States. The review compiled academic, private-sector, and government perspectives to create a cyber security action plan. The plan is to be led by a Cybersecurity Czar, appointed by the President.

---

178. Id.
179. President William J. Clinton & Vice President Albert Gore, Jr., Framework for Global Electronic Commerce (July 1, 1997), http://isis.ku.dk/kurser/blob.aspx?feltid=196532 (recognizing that the Internet is being used to reinvent government and reshape lives and communities, and determining that government can aid in facilitating the growth of commerce on the Internet by taking certain actions).
180. Id.
berspace Policy Review echoes the undertones of the Clinton and Gore Framework, calling for awareness and education, a partnership between the private sector and the government and the international community, and encouraging innovation.\textsuperscript{184}

Additionally, the Department of Justice has suggested that the growth of electronic commerce is likely to be encumbered if consumers have doubts regarding the security of personal information they are entrusting to electronic merchants.\textsuperscript{185} The growth of e-commerce will be hindered if advertisers do not trust the online advertising system in place.

A national-level coordination with the Federal Trade Commission and other agencies, as well as more locally oriented task forces or specialized enforcement units, should work together to combat fraud and deception in global e-commerce by using all available methods, including criminal sanctions, civil penalties, and forfeiture.\textsuperscript{186} If the United States is to be successful in addressing fraud in global e-commerce, it must do so by seeking cooperative solutions with other countries.\textsuperscript{187}

An initiative against click fraud involving countries with Internet and e-commerce structures similar to that of the United States may help successfully conquer click fraud.\textsuperscript{188} These countries may broaden their outreach by systematically including other countries whose Internet usage may not parallel that of the United States.\textsuperscript{189}

Because of the advanced technological nature of click fraud, the initiative may include government officials and industry leaders within the country.\textsuperscript{190} Because the Internet allows for anonymity and makes international boundaries invisible, the existence of countries that tolerate or foster fraud within their borders could undermine even the most carefully developed multinational enforcement scheme.\textsuperscript{191} Any approach should discourage, to the greatest extent possible, the creation of fraud havens and encourage the

\begin{itemize}
  \item strengthening current and future telecommunications and cyber vulnerabilities, and responding to or proactively addressing entities that wish to steal or manipulate protected data on secure federal systems. \textit{Id.} The CNCI consisted of twelve “mostly” classified projects to improve the defense of government computer networks. Nakashima, \textit{supra}.
  \item See \textit{Cyberspace Policy Review, supra} note 181.
  \item \textit{Id.}
  \item \textit{Id.}
  \item \textit{Id.}
  \item \textit{Id.}
  \item \textit{Id.}
  \item Id.
\end{itemize}
maximum amount of information passed to consumers when they are dealing with companies located in such countries.\textsuperscript{192}

An additional method to address the internationality of click fraud is to use Mutual League Assistance Treaties (MLAT).\textsuperscript{193} MLATs have been used in the past where the United States has negotiated with various foreign countries to provide a formal framework for obtaining information and evidence for use in criminal law enforcement matters available only through compulsory measures.\textsuperscript{194}

\textbf{IV. CONCLUSION}

Based on current click fraud technology, search engine self-regulatory measures, increased consumer knowledge, click fraud experts, opinions of lawyers and legislators, the brief history of the issue in the court system, and research regarding past Internet-affiliated initiatives, the future of click fraud lies in the swiftness and severity of action taken by coordinated efforts of the public, private industry, and the government. A criminal solution must be realistic, enforceable, forward-thinking, and widespread. It must be narrow enough to encompass the specific nature of click fraud while remaining broad enough to allow companies, like Google, to continue to create unhindered new technology.

A criminal solution must also be flexible enough to withstand constant advancements, loopholes, and the unpredictable nature of the Internet. It must change, yet remain standardized so that legal precedents and statutory language may be applied to resolve legal disputes. Click fraud should be attacked by alternative approaches—circumventing the issue through litigation instead of merely using civil causes of action that are not specifically tailored. It is not the precise language of the federal criminal statutes that will condemn click fraud, but rather the interpretation of those statutes. Click fraud victims are entitled to restitution for their losses, but because of the importance of e-commerce in our society, criminal sanctions are necessary to promote the public welfare and deter future misconduct.

\textsuperscript{192} \textit{Id.}
\textsuperscript{193} An MLAT is a legally binding treaty that creates obligations for supervisors to exchange information on individuals and to assist in investigations undertaken by other authorities. Kern Alexander, et al., Global Governance of Financial Systems: The International Regulation of Systemic Risk 53 (2006).
\textsuperscript{194} Robinson, Letter to FTC, supra note 185.
Amy Tracy*

* J.D. candidate May 2010; B.A. in journalism and government from Evangel University, 2007. The author wishes to thank the UALR Law Review editorial board, membership, and associate editor, Whitney Foster, for their diligent edits and suggestions in the publication process. The author is grateful for Professor Terrence Cain's legal writing instruction, guidance, and encouragement to apply the more creative aspects of the law. Finally, the author would like to thank Brett Tracy for his input, encouragement, and support in writing this note and in life.