CHARLES C. MANN JAN 1, 2006 12:00 PM

How Click Fraud Could Swallow the Internet

Pay-per-click advertising is big, big, big business. So are bogus hits on Internet ads. It's search giants against scam artists in an arms race that could crash the entire online economy.

STUART CAUFF LAUNCHED a charter-jet service in Miami Beach back in 2002. Being a 21st-century business, JetNetwork advertised on the Internet, especially on search engines. Anyone who Googled, say, "air charter Miami" would be greeted with the familiar list of search results and, in a separate place, a plain box of text with a blue hyperlink to JetNetwork's Web site.

Search ads were perfect for Cauff's business. His potential customers – a diverse group of celebrities, photojournalists, medical evacuees, and people who just needed to get away from or to Miami in a hurry – were scattered across the country. To reach this audience with traditional advertising, he would have had to buy time

Still, the ads were expensive. This kind of advertising is known as pay-per-click, because advertisers shell out money to a search engine every time a surfer clicks on their links. The price and placement depend mainly on how much the advertiser wants to bid for the search term - also known as the keyword in ad jargon. As other charter-air companies began PPC advertising, the cost of a click on a top-ranked ad rose to about $10 - in some cases as high as $30 - and there could be hundreds of clicks a month.

Which is why Cauff was infuriated when he discovered that up to "40 percent, maybe more" of the clicks on his keyword ads apparently came not from potential customers around the nation but from a single Internet address, one that belonged to a rival based in New York City. "If we get clicked fraudulently, it uses up our ad budget," he says. Advertisers usually set limits on how much they will spend, and search engines drop ads once they hit that limit. As a result, fraudulent clicking "literally pushes us off the page," Cauff explains. "And then our competition buys in at a lower price when we're not there."

Cauff was a victim of "click fraud," the illicit manipulation of keyword-based advertising. In this case, the scam appeared straightforward - one company clicked on a rival's search engine ads to drive up its costs. More complex is a second type of bogus ad click that exploits a second form of PPC advertising: ads fed to Web sites - anything from personal blogs to the sites of major corporations - by search providers like Google, Yahoo!, LookSmart, and, soon, MSN. The search engine indexes the content of the Web site and matches it with a group of relevant ads. (The most familiar form is Google's AdSense program - the sets of links labeled *ads by goooooogle* that show up on pages across the Internet. The advertisements that appear on Google itself are part of a separate but related program called AdWords.) Thus, bloggers who write about their air-travel experiences and choose to host such ads may find links on their pages for JetNetworks and its brethren. If a blog visitor

Pay-per-click is the fastest-growing segment of all advertising, reports the Interactive Advertising Bureau. Last year, Yahoo! alone ran more than 250 million individual listings, according to Michael Egan, the company's search-marketing director of content strategy. Yahoo! doesn't break out PPC earnings separately in its financial statements, but Goldman Sachs analyst Anthony Noto believes that keyword advertising accounted for about half of the company's estimated $3.7ébillion in revenue for 2005. PPC is even more lucrative for Google. According to Noto, Google will end 2005 with $6.1 billion in revenue. About 99 percent of that revenue comes from keyword ads (over 56épercent from AdWords, according to the company's most recent quarterly financial statement, and 43épercent from AdSense), making Google a bigger recipient of ad dollars than any television network or newspaper chain. All of which is to say that little blue text links, a type of advertising that barely existed five years ago, are poised to become the single most important form of marketing in the US - unless click fraud ruins it.

If that occurs, the consequences will be felt throughout the Net. By splitting revenue with the sites that host the ads, search engines have become, in effect, the Internet's venture capitalists, funding the content that attracts people to the computer screen. Unlike the VCs who backed the boom-era Internet, search engines now provide revenue to thousands of wildly diverse sites at little up-front cost to them -éPPC advertising is one of the few income sources available to bloggers, for instance. If rampant click fraud overwhelms the system, it will muffle the Internet's fabulous cacophony of voices.

The amount of click fraud is difficult to quantify; estimates of the proportion of fake clicks run from as low as 1 in 10 to as high as 1 in 2. In a widely cited recent study,

deploying complex software to disguise the origins of clicks. For now, the search companies and many of their clients maintain that the problem on their networks is under control. But some observers, like Holcomb, believe that click fraud is "a billion-dollar mess" that "has the potential of destroying the entire industry."

Last October, Boris Elpiner noticed something odd about the Web traffic coming to his company from its PPC ads. As vice president of marketing for RingCentral, an online telecommunications firm in San Mateo, California, Elpiner is in charge of its affiliate-ad program, which hired Yahoo! to distribute RingCentral's ads onto Web sites with compatible content. Poring over his records, he discovered that a keyword term ("fax software download") that had previously generated almost no clicks was suddenly pulling them in. The total cost to RingCentral for the clicks – $2,500 over about four weeks – "was significant, but not immediately noticeable."

Puzzled by the sudden change, Elpiner investigated further. When users visit a Web site, the site server notes the URLs from which they came, the visitors' IP addresses, and other data. Cauff, the charter-jet executive, had used such information to conclude that a competitor was clicking repeatedly on his ads. In this case, Elpiner didn't see an obvious pattern. At the same time, the URLs and IP addresses associated with the suspect clicks "didn't make any sense," he says. "Some of the URLs were error 404 messages, and a lot of the addresses didn't exist."

Elpiner took the matter to Yahoo!, whose analysts "figured it all out quickly," he says. One or more Yahoo! affiliates may have generated deceptive clicks on ads served to their sites, using special software to disguise the source. The scammers, he says, "were clever enough not to take a whole lot from [the ads on] one site, but must have been trying to siphon off a little from many advertisers." Yahoo! gave Elpiner full credit. But it did not, as far as he could tell, try to identify the perpetrators. Instead, Yahoo! and other PPC companies are responding to click fraud by deploying new antifraud technologies. For example, Yahoo! analysts have created click fraud

Although Google and Yahoo! will not, for security reasons, discuss their methods in detail, the advertisements themselves offer some clues. When affiliates sign up for a box of, say, Google ads, they are essentially hosting within their own Web page a small, separate page with its own, very long URL. According to Joseph Tierney, an Internet marketer in central Florida who describes himself as a repentant click fraudster, that URL is embedded with a string of information including the time, in milliseconds; the last time the host Web page was updated, also in milliseconds; and other data used to track customer behavior. Analysts could use this material to match the various time stamps against one another, as well as other information provided by server logs. "If someone from such-and-such IP address clicks on the same ad four times in a second," says Elias Levy, a security architect at Symantec, "you can know that at least three of those clicks don't mean anything. It's inconceivable that Google wouldn't be looking at this."

The company won't confirm it, though. "We don't discuss our techniques," says Shuman Ghosemajumder, a Google business product strategy manager. Nor will Google disclose whether invalid clicks are common or whether it has "a lot" or "just a few" researchers working on click fraud. "We have recognized invalid clicks as a serious problem from the beginning," Ghosemajumder says. "We've done a good job at being effective with these issues in the past, and we believe we will be effective in the future." In his view, PPC companies should be judged not by whether they have succeeded in stamping out click fraud but by whether their advertisers are satisfied.

Not every customer comes away satisfied, though. Last summer Nathan McKelvey, president of the rent-a-jet firm CharterAuction.com in Quincy, Massachusetts, discovered an old server in his office with records of every visitor to his company's Web site since 2002. Many of the visits came through Google's and Yahoo!'s PPC programs. But a substantial number of those clicks came from Denmark, a country where CharterAuction did "exactly zero" of its business. When McKelvey asked

divulge further information. Google won't comment on specific actions with clients; Yahoo! says it is investigating the charges.

PPC companies may have to become more transparent to retain customer confidence, because click fraud has mutated into new, more complex forms. Responding to the demand for fake clicks, shady firms in India created click farms, facilities in which marginally employed people click on advertisements round the clock (these seem to have diminished in number or gone underground since 2004, when the *Times of India* revealed their existence). Companies also have begun attacking rivals with "impression fraud" – repeatedly reloading a search engine page where the rival's ad appears, without clicking on it, in order to eliminate it. (Google and Yahoo! routinely take steps to drop nonperforming ads.) In 2004, a programmer named Michael Bradley allegedly wrote click fraud software that disguised clicks' origins. He was arrested by the Secret Service and charged with attempting to extort $100,000 from Google by threatening to release the software on the Internet; a trial is pending. The action did not eliminate this kind of software – it is now readily available on the Net.

Other enterprising scammers manipulate the affiliate system by creating phony blogs – spam blogs, or splogs – that automatically generate content by continually copying bits from other Web sites, mixing in popular keywords, then signing up the resulting mélange as a Google or Yahoo! affiliate. By using software to link themselves repeatedly to well-known real blogs, splogs trick search engines into listing them high on their results list, thus generating traffic, which in turn generates ad clicks. When unsuspecting Internet searchers visit splogs, they end up clicking the ad links in a frustrated attempt to find some coherent text. Thousands of splogs exist, snarling the blogosphere – and the search engines that index it – in spam.

these boxes continuously send spam, transmit worms and viruses, participate in denial-of-service attacks, and execute a host of other antisocial tasks. These zombie networks can be enormous. In October, Dutch police charged three young men with controlling an incredible 1.5 million computers. In recent months, the owners of zombie networks have begun turning to click fraud -éwith "very effective" results, according to Tierney, the former click frauder. The robot machines create clicks from all around the world at apparently random intervals, making them difficult to identify.

But even if zombie click fraud becomes common, the damage can probably be contained as long as its targets are limited to individual advertisers. As Symantec's Levy points out, PPC firms can always give the victims their month's service free - reducing click fraud to a type of overhead, a cost of doing business. But the impact would be much larger, he notes, if someone decided to attack not single companies but the PPC system itself. "It would not be difficult to construct a worm that would go through the Net, clicking on every Google or Yahoo! affiliate ad that it saw," Levy says. "If enough of these were loose, you'd swamp the entire system in noise - millions or even billions of extra clicks. It would be very hard to defend against."

Is this likely to happen? "I would like to be able to say that people aren't that stupid or greedy or aggressive or mindless," says Chase Law's Butler. "But I can't say any of those things. That is definitely the threat - a threat to the entire system by somebody who is just doing it for the hell of it."

Type "click fraud" into a search box and you get links to more than 30 million Web sites and ads for the dozens of companies that have sprung up to help victims track the practice. Down the right-hand side of the page march the ad links: Click Defense, Clicklab, Clickrisk, ClickAssurance, VeriClix, Authenticlick, WhosClickingWho. Stoking advertisers' fears by claiming that the system is drowning in click fraud, these outfits nonetheless solicit clients with ... keyword ads

Most of these firms simply provide ways for advertisers to outsource the tedious task of examining internal logs for fraud. Among those trying to do more is Visitlab, in Santa Cruz, California. According to CEO Vikas Kedia, Visitlab's clients channel incoming clicks through his company, which screens them with software tailored for each customer. The software, now in beta, consists of modules that look for telltale behavior - the use of a proxy server, say, or clicks coming from geographic areas that are unlikely to have customers. By amassing data on click behavior and constantly adjusting the software, Kedia believes, it should eventually be possible to detect even a single fraudulent click. "Google could do all this," he says. "But nobody is sure whether to trust them. We're a third party."

Bill Gross, the man who invented PPC back in the late '90s when he presided over the startup incubator Idealab, has argued that, despite the cleverness of the various methods used to fight it, click fraud will continue to cast a shadow over PPC advertising. Ultimately, he believes, advertisers will switch to another model, which he calls cost-per-action (others use terms like cost-per-transaction or cost-per-acquisition). Whatever the name, though, advertisers pay only when a click results in a specified action, such as a sale or a Web site registration. Gross started a CPA search engine, Snap.com, in late 2004. When customers enter the term "airline tickets" on the site, ads for airlines appear. But those airlines don't pay Snap a penny until someone who clicks the ad actually buys a ticket. Even if scammers used zombie networks, the system would ignore them, because it charges only for clicks that lead to an action. Snap, still in beta, is not exactly roaring ahead: According to its own statistics, the firm has 2,300 CPA advertisers. That's roughly 2 percent of Google's or Yahoo!'s advertising base.

Yahoo! is not looking into cost-per-action, Egan says, because such a system requires businesses to share sensitive cost data with their advertising partners. "We

A possible answer to the privacy worries may be something called Google Wallet. This new initiative, not yet unveiled as of early December, is believed to be a payment scheme that surfers would use, for example, when they bought something after clicking on a Google ad. In theory, at least, Google could process the payment to the advertiser without having to know anything about its costs, profit margins, or other sensitive data. Like Gross's cost-per-action, Google Wallet would be immune to click fraud - zombie machines could click away, and the system would simply ignore them.

Nobody thinks that these measures will eliminate click fraud. Keyword advertising - especially on affiliates - will continue to grow, making it an ever more inviting target to the Net's legion of bad actors. All the while, PPC will continue to be vulnerable to attacks by blackhats who want to disrupt the system as a whole, rather than defraud the individual companies that use it. In consequence, PPC providers seem doomed, at least for the near future, to an endless race against the scammers, spammers, and network jammers. "If you'd told me five years ago that I would be talking about 'fake clicks,' I would have told you that you were crazy," says John Slade, who leads Yahoo!'s click protection efforts. "Now it's all I spend my time on."

Contributing editor Charles C. Mann (www.charlesmann.org) **is the author of* 1491: New Revelations of the Americas Before Columbus.**
credit Mirko Ilic