click fraud

The dark side of online advertising

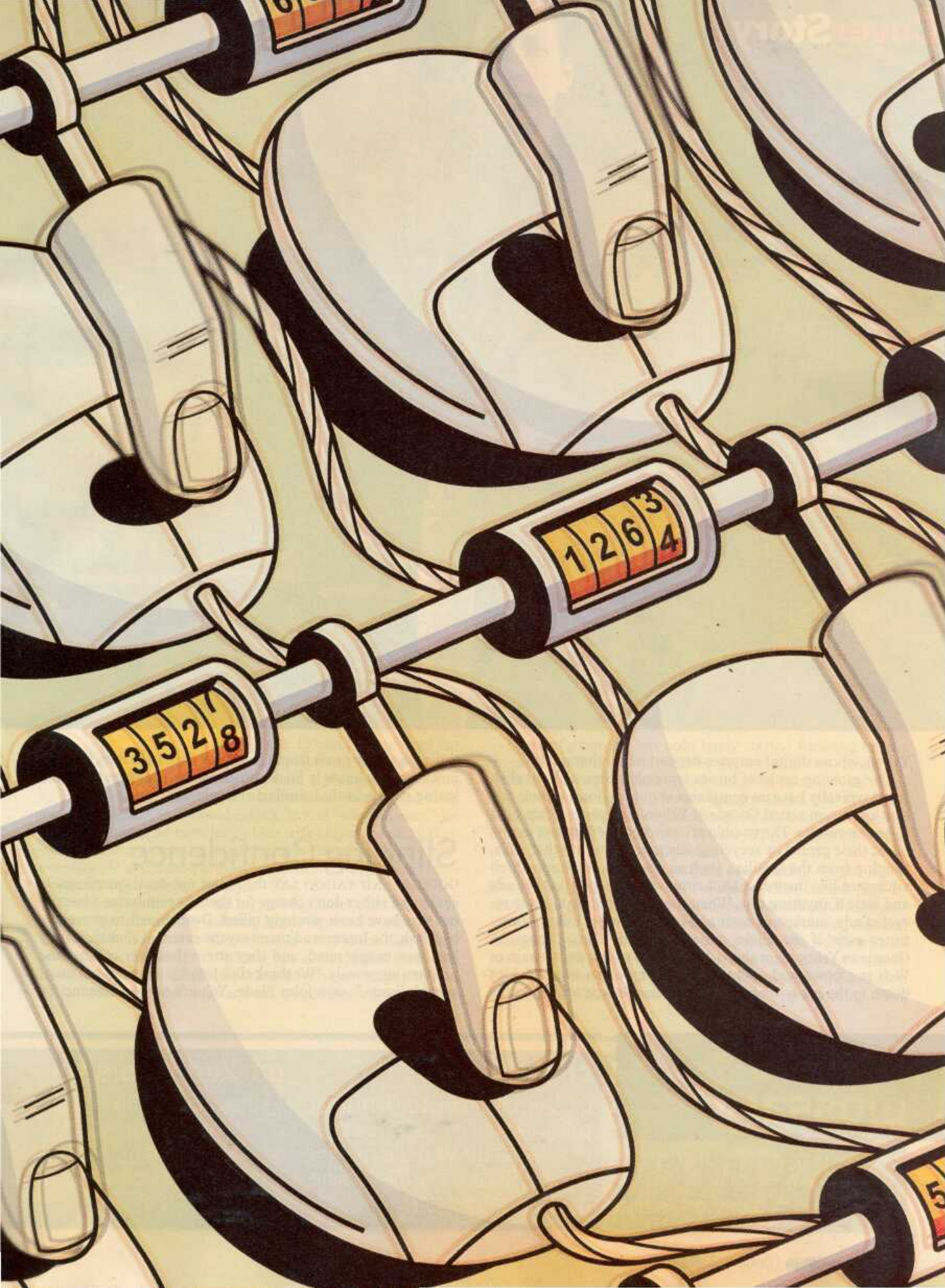
By Brian Grow and Ben Elgin

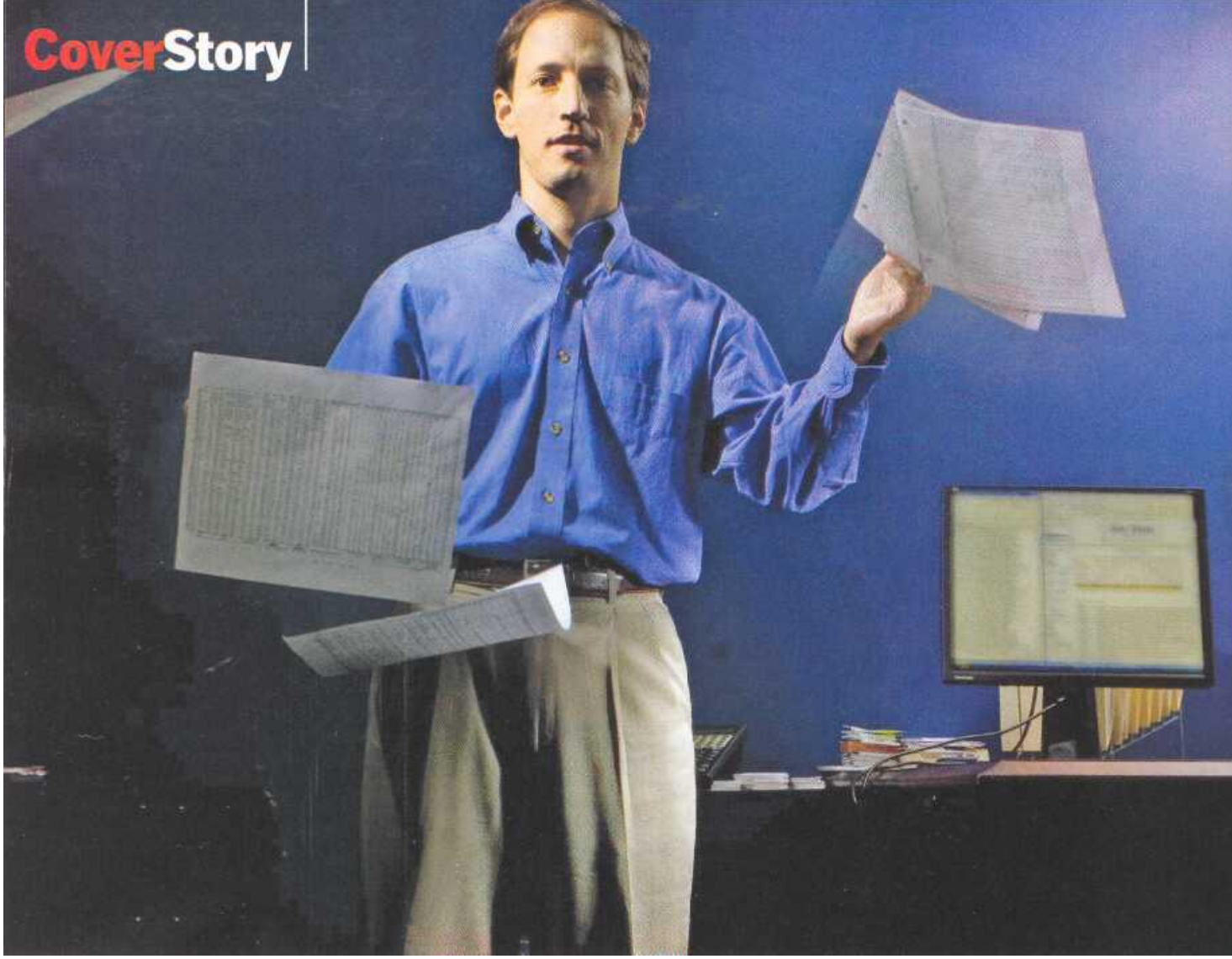
Martin Fleischmann put his faith in online advertising. He used it to build his Atlanta company, MostChoice.com, which offers consumers rate quotes and other information on insurance and mortgages. Last year he paid Yahoo! Inc. and Google Inc. a total of $2 million in advertising fees. The 40-year-old entrepreneur believed the celebrated promise of Internet marketing: You pay only when prospective customers click on your ads.

Now, Fleischmann's faith has been shaken. Over the past three years, he has noticed a growing number of puzzling clicks coming from such places as Botswana, Mongolia, and Syria. This seemed strange, since MostChoice steers customers to insurance and mortgage brokers only in the U.S. Fleischmann, who has an economics degree from Yale University and an MBA from Wharton, has used specially designed software to discover that the MostChoice ads being clicked from distant shores had appeared not on pages of Google or Yahoo but on curious Web sites with names like insurance1472.com and insurance060.com. He smelled a swindle, and he calculates it has cost his business more than $100,000 since 2003.

Fleischmann is a victim of click fraud: a dizzying collection of scams and deceptions that inflate advertising bills for thousands of companies of all sizes. The spreading scourge poses the single biggest threat to the Internet's advertising gold mine and is the most nettlesome question facing Google and

HARRY CAMPBELL


1 2 6 3 4
3 5 2 7 8



Yahoo, whose digital empires depend on all that gold.

The growing ranks of businesspeople worried about click fraud typically have no complaint about versions of their ads that appear on actual Google or Yahoo Web pages, often next to search results. The trouble arises when the Internet giants boost their profits by recycling ads to millions of other sites, ranging from the familiar, such as cnn.com, to dummy Web addresses like insurance1472.com, which display lists of ads and little if anything else. When somebody clicks on these recycled ads, marketers such as MostChoice get billed, sometimes even if the clicks appear to come from Mongolia. Google or Yahoo then share the revenue with a daisy chain of Web site hosts and operators. A penny or so even trickles down to the lowly clickers. That means Google and Yahoo at times passively profit from click fraud and, in theory, have an incentive to tolerate it. So do smaller search engines and marketing networks that similarly recycle ads.

Slipping Confidence

GOOGLE AND YAHOO SAY they filter out most questionable clicks and either don't charge for them or reimburse advertisers that have been wrongly billed. Determined to prevent a backlash, the Internet ad titans say the extent of click chicanery has been exaggerated, and they stress that they combat the problem vigorously. "We think click fraud is a serious but manageable issue," says John Slade, Yahoo's senior director for

rogues glossary

The murky world of Web advertising has its own jargon

click fraud
Clicking on Internet advertising solely to generate illegitimate revenue for the Web site carrying the ads; those doing the clicking typically also get paid.

parked web site
A site typically with little or no content except for lists of Internet ads, often supplied by Google or Yahoo; many of them are the source of false clicks.

FLEISCHMANN estimates fraud has cost his Atlanta company $100,000

global product management. "Google strives to detect every invalid click that passes through its system," says Shuman Ghosemajumder, the search engine's manager for trust and safety. "It's absolutely in our best interest for advertisers to have confidence in this industry."

That confidence may be slipping. A *BusinessWeek* investigation has revealed a thriving click-fraud underground populated by swarms of small-time players, making detection difficult. "Paid to read" rings with hundreds or thousands of members each, all of them pressing PC mice over and over in living rooms and dens around the world. In some cases, "clickbot" software generates page hits automatically and anonymously. Participants from Kentucky to China speak of making from $25 to several thousand dollars a month apiece, cash they wouldn't receive if Google and Yahoo were as successful at blocking fraud as they claim.

"It's not that much different from someone coming up and taking money out of your wallet," says David Struck. He and his wife, Renee, both 35, say they dabbled in click fraud last year, making more than $5,000 in four months. Employing a common scheme, the McGregor (Minn.) couple set up dummy Web sites filled with nothing but recycled Google and Yahoo advertisements. Then they paid others small amounts to visit the sites, where it was understood they would click away on the ads, says David Struck. It was "way too easy," he adds. Gradually, he says, he and his wife began to realize they were cheating unwitting advertisers, so they stopped. "Whatever Google and Yahoo are doing [to stop fraud], it's not having much of an effect," he says.

Spending on Internet ads is growing faster than any other sector of the advertising industry and is expected to surge from $12.5 billion last year to $29 billion in 2010 in the U.S. alone, according to researcher eMarketer Inc. About half of these dollars are going into deals requiring advertisers to pay by the click. Most other Internet ads are priced according to "impressions," or how many people view them. Yahoo executives warned on Sept. 19 that weak ad spending by auto and financial-services companies would hurt its third-quarter revenue. Share prices of Yahoo and Google tumbled on the news.

Google and Yahoo are grabbing billions of dollars once collected by traditional print and broadcast outlets, based partly on the assumption that clicks are a reliable, quantifiable measure of consumer interest that the older media simply can't match. But the huge influx of cash for online ads has attracted armies of con artists whose activities are eroding that crucial assumption and could eat into the optimistic expectations for online advertising. (Advertisers generally don't grumble about fraudulent clicks coming from the Web sites of traditional media outlets. But there are growing concerns about these media sites exaggerating how many visitors they have—the online version of inflating circulation.)

The success of Google and Yahoo is based partly on the idea that clicks are reliable

Most academics and consultants who study online advertising estimate that 10% to 15% of ad clicks are fake, representing roughly $1 billion in annual billings. Usually the search engines divide these proceeds with several players: First, there are intermediaries known as "domain parking" companies, to which the search engines redistribute their ads. Domain parkers host "parked" Web sites, many of which are those dummy sites containing onljr ads. Cheats who own parked sites obtain search-engine ads from the domain parkers and arrange for the ads to be clicked on, triggering bills to advertisers. In all, $300 million to $500 million a year could be flowing to the click-fraud industry.

Law enforcement has only lately started focusing on the threat. A cybercrime unit led by the FBI and U.S. Postal Inspection Service just last month assigned two analysts to examine whether federal laws are being violated. The FBI acted after noticing suspected cybercriminals discussing click fraud in chat rooms. The staff of the Senate Judiciary Committee has launched its own informal probe.

Many advertisers, meanwhile, are starting to get antsy. Google and Yahoo have each settled a class action filed by marketers (page 52). In late September a coalition of such major brands as InterActive Corp.'s Expedia.com travel site and mortgage broker LendingTree is planning to go public with its mounting unease over click fraud, *BusinessWeek* has learned. The companies intend to form a group to share information and pressure Google and Yahoo to be more forthcoming. "You

paid-to-read
A PTR site pays members to look at other Web sites and offers from marketers; often used to generate fake clicks on parked Web sites.

clickbot
Software that can be used to produce automatic clicks on ads; some versions employed in click fraud can mask the origin and timing of clicks.

botnet
A collection of computers infected with software that allows them to be operated remotely; networks of thousands of machines can be used in click fraud.

can't blame the advertisers for being suspicious," says Robert Pettee, search marketing manager for LendingTree, based in Charlotte, N.C. "If it's your money that's going out the door, you need to be asking questions." He says that up to 15% of the clicks on his company's ads are bogus.

In June, researcher Outsell Inc. released a blind survey of 407 advertisers, 37% of which said they had reduced or were planning to reduce their pay-per-click budgets because of fraud concerns. "The click fraud and bad sites are driving people away," says Fleischmann. He's trimming his online ad budget by 15% this year.

Google and Yahoo insist there's no reason to fret. They say they use sophisticated algorithms and intelligence from advertisers to identify the vast majority of fake clicks. But the big search engines won't disclose the specifics of their methods, saying illicit clickers would exploit the information.

Some people who have worked in the industry say that as long as Google and Yahoo distribute ads to nearly anyone with a rudimentary Web site, fraud will continue. "Advertisers should be concerned," says a former Yahoo manager who requested anonymity. "A well-executed click-fraud attack is nearly impossible, if not impossible, to detect."

DAVID AND RENEE STRUCK set up dummy Web sites with recycled ads

PHOTOGRAPH BY THOMAS STRAND; ILLUSTRATIONS BY HARRY CAMPBELL

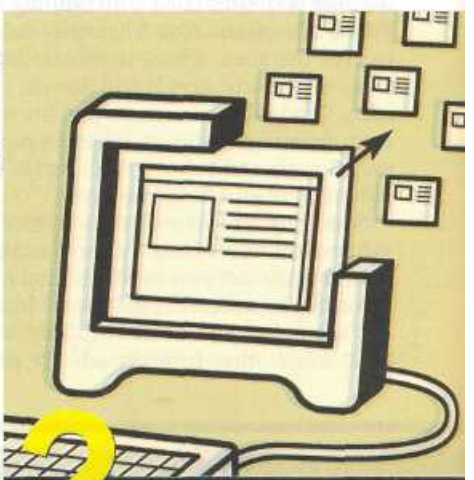
ALTHOUGH 5 FEET 6 AND 135 POUNDS, Marty Fleischmann is no one to push around. He barked orders at much bigger oarsmen while serving as coxswain on the varsity crew team at Yale in the mid-1980s. His shyness deficit surfaced again when he later played the role of Jerry Seinfeld in the student follies at Wharton. Married and the father of three children, he tends to pepper his conversation with jargon about incentives and efficiencies.

Before he and partner Michael Levy co-founded their financial-information company in 1999, Fleischmann worked in Atlanta at the management consulting firm A.T. Kearney Inc., advising major corporations in the shipping and pharmaceutical

follow the money

Click fraud schemes vary and often involve a complicated chain of relationships. Here's one way the process can work:

1 XYZ Widgets signs up with Google or Yahoo to advertise on the Internet, agreeing to pay the search engine every time somebody clicks on an XYZ ad.



2 Google or Yahoo displays the ad on its own site but also recycles it to millions of affiliates, including "domain parking" companies.

industries. One lesson he says he learned is that big companies are loath to cut off any steady source of revenue. Google and Yahoo are no different, he argues.

That cynicism several years ago contributed to MostChoice's assigning an in-house programmer to design a system for analyzing every click on a company ad: the Web page where the ad appeared, the clicker's country, the length of the clicker's visit to MostChoice's site, and whether the visitor became a customer. Few companies go to such lengths, let alone companies with only 30 employees and revenue last year of just $6.4 million.

To Fleischmann, the validity of his clicks, for which he pays up to $8 apiece, has become an obsession. Every day he pores over fresh spreadsheets of click analysis. "I told Yahoo years ago," he says," 'If this was costing you money instead of making you money, you would have stopped this.'"

Google, he says, does a better job than Yahoo of screening for fraud. But neither adequately protects marketers, he argues. Until March, 2005, Google, based in Mountain View, Calif., charged advertisers twice for "double clicks," meaning those occasions when a user unnecessarily clicks twice in quick succession on an ad. Confirming this, Google's Ghosemajumder says that before the company made the change, it felt it had to focus "on issues of malicious behavior," though now it identifies double clicks and bills for only one.

Korean Clones

FLEISCHMANN'S DAILY IMMERSION in click statistics fuels his indignation. How, he wants to know, did he receive traffic this summer from PCs in South Korea which are clicking on insurancel472.com and insurance060.com? The only content on these identical sites—and five other clones with similar names-are lists of Yahoo ads, which occasionally have included

"If this was costing [Yahoo] money instead of making it," they would have stopped it

MostChoice promotions. Fleischmann's spreadsheets revealed, not surprisingly, that all of the suspected Korean clickers left his site in a matter of seconds, and none became customers. The two individuals registered as owning the mysterious insurance sites are based in South Korea. They didn't respond to requests for comment, and most of the sites disappeared in late summer, after MostChoice challenged Yahoo about them.

Fleischmann, like most other advertisers, has agreed to let Google and Yahoo recycle his ads on affiliated sites. The search engines describe these affiliates in glowing terms. A Google "help" page entitled "Where will my ads appear?" mentions such brand names as AOL.com and the Web site of *The New York Times.* Left unmentioned are the parked Web sites filled exclusively with ads and sometimes associated with click-fraud rings.

Google and Yahoo defend their practice of recycling advertising to domain-parking firms and then on to parked sites, saying that the lists of ads on the sites help point Internet surfers toward relevant information. Google notes that it allows advertisers to identify sites on which they don't want their ads to run.

But this Google feature doesn't apply to many parked sites, and Yahoo doesn't offer the option at all. In any event, excluding individual sites is difficult for marketers that don't do the sort of time-consuming research MostChoice does. Whether they know it or not, many other companies are afflicted in similar ways. At *BusinessWeek's* request, Click Forensics Inc., an online auditing firm in San Antonio, analyzed the records of its 170 financial-services clients and found that from March