

BENJAMIN EDELMAN

## Assessing and Improving the Safety of Internet Search Engines

### 1. Overview

Where Internet users go, attackers follow. Users embrace e-mail; then spammers fill their inboxes with junk mail. With the rise in online commerce, phishers trick them into giving up their passwords. Users find handy downloadable applications; adware vendors bundle them with pop-up-spewing add-ons.

The rise of Internet search brings a new type of risk. Hostile Web sites might seek to harm users or take advantage of them – whether through spyware, spam, scams, or other bad practices – because search engines often do not filter these sites from their results. Consider this scenario:

Suzy wants to perform Beyonce's *Crazy in Love* for her school talent show. To make sure she dresses the part, she performs a Google search for <celebrity photos>. When she clicks the first search result, [celebritypictures.duble.com](#), she is quickly prompted to install an adware-bundled ActiveX control in order to browse the site's contents. Eager to view photos of her celebrity role model, she accepts the installation of a new browser toolbar and a pop-up serving adware program.

In principle, search engines' listing rules, ranking rules, and advertising policies might shield users from some bad practices, and users' good judgment could protect them from others. But empirically, search engines often lead users to dangerous content. My analysis of search engine safety finds bad practices among approximately 5% of search results for popular keywords, or roughly one site per page of search results.

The rise of paid search results brings additional complications: Profit motivations have shifted search engines’ ranking methodologies. Prominent results often reflect solely a site’s willingness to pay rather than its quality, relevance, or safety.

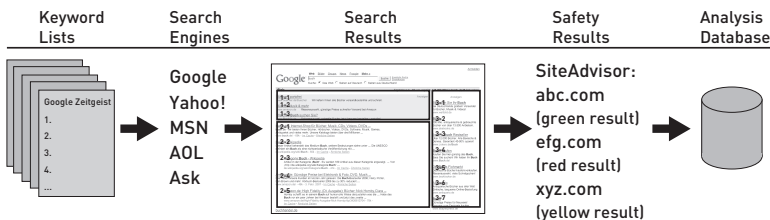
## 2. Methodology

The empirical section of this paper is based on work previously conducted jointly with Hannah Rosenbaum and previously posted as *The Safety of Internet Search Engines* (2006). The online version of that article includes additional data and appendices.

To compare the safety of search engines’ listings, we compiled 1,394 popular keywords using lists of common searches from Google Zeitgeist, Yahoo!, AOL, Lycos, Wordtracker, and other industry sources (cf. figure 1). Some lists included adult search terms, which we excluded to maintain consistent keyword content. We considered the first five pages of results for each keyword from each of the five biggest search engines: Google, Yahoo!, AOL, MSN, and Ask.

We analyze search engine results, noting which sites were listed where (by search engine, keyword, page, position) and how they were labeled (organic versus sponsored). We assess the safety of listed sites by consulting SiteAdvisor’s Web safety database. SiteAdvisor is an Internet security company that protects users from hostile web sites by measuring and reporting web site safety. SiteAdvisor safety ratings are based on automated tests that analyze Web sites for exploits, downloads containing spyware, adware, or other unwanted programs, pop-ups, links to dangerous sites, and e-mail submission forms. SiteAdvisor’s automated tests are

FIGURE 1  
Methodology of Analysis



supplemented by feedback from volunteer reviewers, comments from Web site owners and input from SiteAdvisor analysts. SiteAdvisor's safety ratings allow us to assess search engines' results along a number of axes, as set out in subsequent sections.

If SiteAdvisor rates a site as ›yellow‹ or ›red‹, typical users will generally be concerned about the safety of the rated site. A red rating warns users that a site poses a security threat, including the misuse of e-mail addresses, scams, exploits, and downloads containing spyware, adware, or other unwanted programs. A yellow rating is given to sites that pass most of SiteAdvisor's safety tests but still employ practices warranting a user to exercise caution. SiteAdvisor's FAQ has details on SiteAdvisor's methods – including more information on the specific problems SiteAdvisor detects, and more on how SiteAdvisor's robots work.

We weight all links equally – reflecting that users tend to treat sponsored and organic links identically (Consumer Reports 2002).

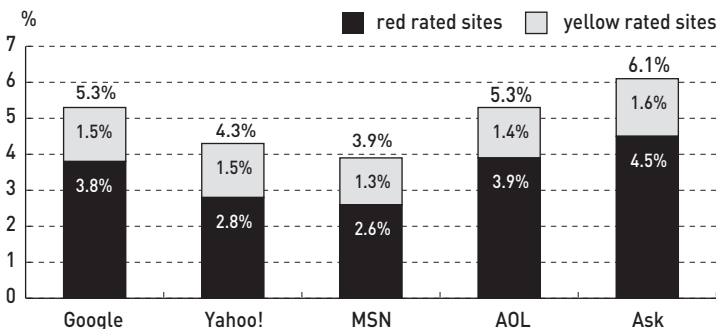
The remainder of this chapter presents notable findings, followed by policy recommendations.

### 3. Comparing Search Engines

Though many users rely on only the top few search engines, there are plenty of other choices (Search Engine Megalist). Existing research tends

FIGURE 2

Percentage of unsafe (›red‹ and ›yellow‹) results by search engine



to focus on users choosing a search engine to obtain the most relevant or useful results. Relevance is a natural way to choose a search engine, but users might also consider choosing a search engine based on safety. After all, even the most relevant results may not be desirable if they bring substantial risks of harm. It is therefore natural to begin by comparing safety of the leading search engines.

Our analysis reveals some significant differences among the major search engines. Overall, our tests show MSN's results to be the safest of the tested search engines (cf. figure 2). This may reflect, at least in part, an explicit publicly-documented MSN effort to remove unsafe sites. Least safe are results at Ask – where unsafe sites are more than 56% more frequent than at MSN (6.1% versus 3.9%).

Search engine safety performance varies across certain subsets of our keyword list. For example, Yahoo! returns a lower percentage of dangerous results when searching for words in the Yahoo! 2005 Top Searches list than when searching for words in Google's Zeitgeist listings. In contrast, Google, AOL, and Ask perform better when searching for Google Zeitgeist keywords as opposed to those in the Yahoo! 2005 Top Searches list. MSN performed consistently for both of these keyword lists. The Yahoo! 2005 Top Searches list contains a higher percentage of celebrity and entertainment terms than the Google Zeitgeist list, implying that Yahoo! is a safer choice for these categories.

More specific keyword subsets reveal greater variance in safety performance. We use Google Zeitgeist to group keywords into categories – lists of five to ten keywords in a variety of categories. MSN ranks safest for 23 out of 63 keyword categories (including ›tabloid fodder‹ and ›video games‹), while Ask only ranks safest for 5 categories (including ›popular sports‹ and ›hot cars‹). Yahoo! proves the safest for ›games‹ keywords (such as ›Halo 2‹ and ›RuneScape‹), while AOL ranks safest for ›digital music‹ keywords (such as ›bittorrent‹ and ›iTunes‹). Google returns the safest results for ›look it up‹ keywords (such as ›lyrics‹ and ›weather‹), but returns the most dangerous results for ›tech toys‹ keywords (such as ›iPod nano‹ and ›Nintendo Revolution‹). See Risky Keywords and Categories (below).

On the whole, we see little basis to conclude that any search engine is much safer than any other; safety rankings vary too much from search to search. But, overall, MSN outperforms the others. We recommend extra caution when searching at Ask.

#### 4. Results in Perspective

At first glance, a 4%-6% incidence of red and yellow sites in search results may not appear alarming. But even a single visit to a dangerous site can have serious and lasting implications for the average Internet user:

Sites using browser exploits can insert unwanted code on a user's PC, which may cause serious security breaches and render a user's PC essentially inoperable. For example, we found exploit site `celebritypro(dot)com` when searching for ›Halle Berry‹ at Google. This site uses security exploits to install software onto a user's PC without the user's consent.

Sites which include downloads with adware or spyware can clutter a user's PC with unwanted programs that serve intrusive advertising pop-ups, track users' browsing habits, and cause operating difficulties. A single download at `ratloaf.com` (found in top search results for ›screensavers‹ at Yahoo!) can come bundled with three different adware/spyware programs.

Sites which misuse personal information can cause endless spam and threaten the safety of financial and other personal information. A single sign-up at `rewardsgateway.com` (found in search results for ›iPods‹ at Google) can lead to 303 e-mails per week.

It is estimated that US Internet users conduct 5.7 billion searches per month (NIELSEN NETRATINGS 2006). Suppose each search yields exactly one click to one of the sites listed in the results. Then even a 5% incidence of red/yellow sites would mean 285 million clicks to these sites every month from search engines.

With spam, adware, and spyware costing consumers and corporations increasing amounts of time and money, we believe that the incidence of red and yellow sites in search engine results is extremely significant and is a contributing factor to the problems of spam, adware, spyware, and other online threats.

#### 5. Organic versus Paid Results

Today's search engines combine two dramatically different kinds of results. Search engines' ›main‹ results are organic listings – search engines' best assessment of what Web pages are most relevant to users' search requests. But search engines also show sponsored listings, where inclusion reflects a site's willingness to pay to be listed (cf. figure 3).

FIGURE 3  
Google organic results (left) and sponsored listings (top, right) for the keyword phrase ›free iPods‹



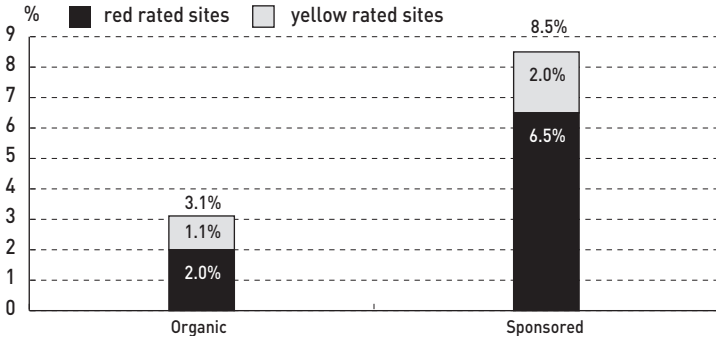
These different kinds of listings yield different risks to users. Organic listings are generally added, selected, and ranked without substantial human involvement; search engines’ automated systems pick and present sites. Without any human evaluating site safety, users might reasonably worry that organic results could take them to unsafe sites.

In contrast, search engines’ sponsored links seem to offer an aura of safety: Search engines post detailed editorial policies as to who may advertise and how (see Google’s Editorial Guidelines and Yahoo!’s Sponsored Search Listing Guidelines.)

Despite these special rules for search engine advertising, our testing indicates that organic sites are, overall, substantially safer than sponsored listings. Take the example of ›free iPods‹, where first page results yield many more red sites in sponsored results compared to organic results (cf. figure 4).

FIGURE 4

Red and yellow sites appear in sponsored results at two to four times the rate of organic results



Across all search terms we analyze, a Google ad is on average more than twice as likely to take a user to an unsafe site than is a Google organic link. At Ask, the difference is especially pronounced: Their sponsored results are almost four times as risky as their organic listings.

We are troubled by the untrustworthiness of search engines' ads. At first glance, search engines' voluminous rules would seem a virtual guarantee of good outcomes. Google's rules are more than 1,900 words long, and Yahoo!'s thousand-plus words include thirty-six distinct bullet-point'ed requirements. Indeed, in some areas, search engines seem to have made strong headway – such as for online pharmacies, where a PharmacyChecker evaluation process assures that only legitimate companies can buy ads (Google's Online Pharmacy Qualification Process). But on the whole, search engines' policies don't squarely speak to the problems at hand. For example, search engines sell ads to sites that send users literally hundreds of e-mails per week. (Included in our search results are *consumerincentivezone.com*, *freegiftworld.com*, and *lookdog.com*.) Search engines also sell ads to sites that infect users' computers with adware programs that open numerous annoying pop-up ads. (Included in our search results are *scenicreflections.com*, *screenscenes.com*, and *totallyfunfreegames.com*.) Search engines' editorial rules largely ignore these practices, and even where they do discuss these issues, enforcement seems to be lax.

In contrast, search engines' organic listings reflect the Web's assessment of the quality and usefulness of a site, as measured by who links

to whom. Spammers, spyware-pushers, and other pariahs may be able to buy search engine ads, but they tend to fare worse in organic listings.

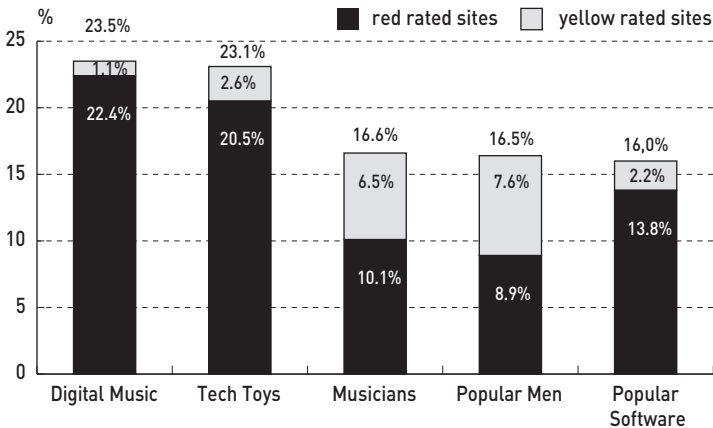
Others have previously noted untrustworthy ads. For example, noted security expert Richard Smith has complained about this problem, after a bogus weather program infected his wife’s computer via a misleading Google ad (*ComputerWorld* 2006).

Why don’t search engines get tough on untrustworthy ads? One explanation is that it’s a difficult task: Search engines lack automated link-based analysis of advertisers’ trustworthiness – the only thing keeping organic results (relatively) safe. If search engines won’t or can’t use link analysis to vet their advertisers, search engines might have to invest staff time in manually determining advertisers’ reputations, and search engines may hesitate to incur the associated costs. Separately, some analysis indicates that search engines make big money selling ads to untrustworthy sites – many millions of dollars each year (EDELMAN 2006a).

### 6. Risky Keywords and Categories

When searching the Web, users face risks that vary dramatically according to what categories they search for. A large proportion of malicious sites

FIGURE 5  
**The incidence of red and yellow sites, within Google results, for five top Google Zeitgeist categories**



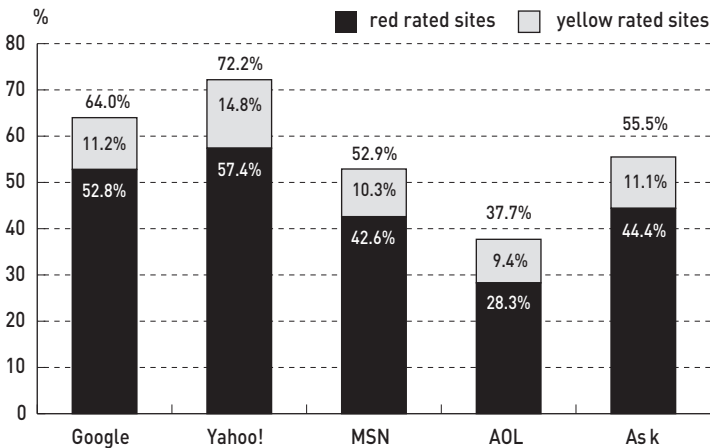
are concentrated in certain high risk categories; searching within these danger zones exposes users to a high probability of ending up in the dark alleys of the Web.

The technology trade press confirms our sense that certain parts of the Web tend to be unsafe. For example, a recent TechTarget article encourages users to avoid spyware by »stay[ing] away from any questionable sites, including pornography, gambling, hacking or other off-beat sites.« Similarly, Security Pipeline tells users to »stay on your guard« when visiting potentially-unsafe domains, such as song-lyric sites, game, and hobby sites.

Our analysis confirms the basic advice of TechTarget and Security Pipeline (cf. figure 5). For example, users searching for digital music at Google face 75 times as many risky sites as users searching for news. (We reach this conclusion by comparing the frequency of unsafe sites within »news outlet« searches, as reported by Google Zeitgeist, with the frequency of unsafe sites within Zeitgeist's »digital music« keyword list.)

Results within categories also differ noticeably between search engines (cf. figure 6), and some search engines are noticeably safer than others for specific categories. For example, only 0.2% of Yahoo! results for Google Zeitgeist »games« keywords are rated red or yellow, compared

FIGURE 6  
**Percentage of red and yellow results for »free screensavers«, the most dangerous search phrase tested**



with 8.9% of AOL results. Unsafe search results for ›movie-related‹ keywords range from 2.5% for MSN to 8.6% for Ask.

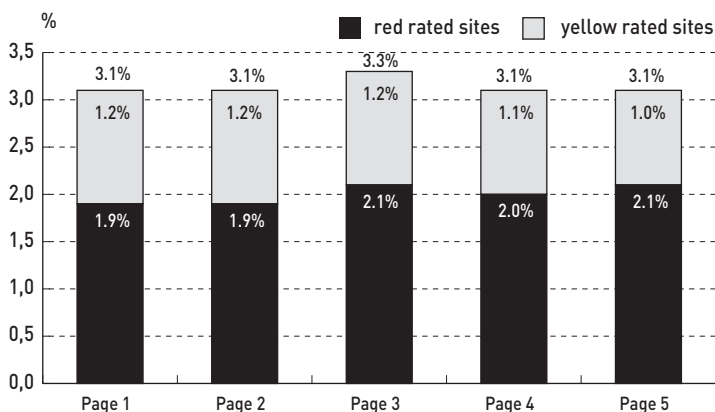
Overall, the most dangerous search term is ›free screensavers‹, which returns results that are 57% red or yellow on average. Search engines differ greatly in their results for this keyword: Yahoo! returns 72.2% red or yellow results, compared with 37.7% at AOL. So users are almost twice as likely to stumble onto a risky screensaver site using Yahoo! versus AOL.

In general, many of the riskier keywords tend to be associated with downloads and file sharing. Google’s top five riskiest keyword searches are ›free screensavers‹ (64.0%), ›Bearshare‹ (57.0%), ›screensavers‹ (54.6%), ›Winmx‹ (50.5%), and ›limewire‹ (46.4%).

Even keywords that are generally not regarded as risky yield relatively high rates of red and yellow sites. A Google search for ›care bears‹ leads to 14.6% red or yellow sites. ›Birthday cards‹ leads to 15.6%, ›south beach diet‹ leads to 14.8%, and ›weather‹ leads to 14.0%.

Our testing confirms the core facts behind standard advice to avoid ›risky‹ categories. But that advice is arguably far from practical (SiteAdvisor 2006). Asking users to give up broad swaths of the Web imposes great limitations and substantial responsibility, while offering little insight as to how to stay safe while nonetheless enjoying the Web. In addition, danger lurks beyond the generally accepted ›risky‹ categories, so users can never really let down their guard.

FIGURE 7  
Page 1 results versus results on pages 2 through 5



## 7. Analysis by Result Page

In an attempt to stick with safe search engine results, some users limit themselves to top results. (See e.g. iProspect 2006, finding that 62% of searchers click a result within the first page of listings.) Lower-ranked sites might not be as good as top sites, users seem to think, so visiting only top sites perhaps offers an appearance of safety. Unfortunately, our analysis indicates that this strategy is largely unjustified.

In our testing, we find little safety benefit from sticking to top search results (cf. figure 7). The first organically ranked results are marginally safer than the tenth results and page 1 results are slightly safer than pages 2 through 5. But the benefit is slight: Google's page 1 results are just 0.05% safer than pages 2-5.

## 8. Search Engine Self-Regulation

Search engines face reputational and other incentives to provide high quality results – a factor that, in principle, might suffice to keep listings safe and blunt the need for policy intervention. Sophisticated users could conceivably evaluate search engine safety and choose a preferred search engine accordingly – scorning any search engine that does too little to keep users safe. On this view, market forces naturally deter search engines from providing unsafe results or, indeed, results undesirable for any other reason.

Yet there is ample reason to doubt the effectiveness of pure private decision-making. As a threshold matter, search engines' private decisions have yielded the results set out above – with many unsafe sites in search engine results, and many users substantially harmed by these unsafe sites. In practice, search engines seem to face little real risk of user dissatisfaction in part because users generally don't know how they got infected or deceived. For example, a user might know he has spam or spyware problems, but typically he would not realize that a search engine played a crucial role in directing him to the site or sites that caused his problems. A user might know he is being charged for a service he didn't want, but the user is less likely to realize that he only signed up for that service thanks to a search engine ad. To the extent that some iota of sophisticated users realize the source of their problems, these users are also probably sophis-

ticated enough to avoid such problems in the first place. With sophisticated users both rare and unconcerned, such users are unlikely to push for search engine safety for everyone else.

Furthermore, the heightened risks of search engines' ads suggest an additional market failure: That search engines benefit financially from including unsafe sites in their result listings. Including a given unsafe site may slightly tarnish a search engine's good name, but it simultaneously earns a search engine an advertising fee. This tension suggests search engines may not always do what would best serve their users.

Because search engines are concerned about their reputations, one might expect search engines to refuse ads that are widely used to criticize search engines' practices. But available facts suggest precisely the opposite: Such ads are growing in prominence, not shrinking. In May 2006, I specifically criticized a Google ad keyed to the keyword ›Skype‹, promoting [download-it-free.com](http://download-it-free.com), a site which tries to charge \$29 for users to download Skype (a free program available without charge from [skype.com](http://skype.com)) (EDELMAN 2006b). My concern was echoed in various news publications that covered the story. Rather than ejecting the advertiser I flagged, Google retained it, and it remains the top advertiser for ›Skype‹ to this day. Furthermore, [freedownloadhq.com](http://freedownloadhq.com), [download-zone-free.com](http://download-zone-free.com), [freedownloadhq.com](http://freedownloadhq.com), and [downloadsglobe.com](http://downloadsglobe.com) all advertise for this same term (among others), making ›Skype‹ results a veritable mine field of scams and rip-offs. If search engines' reputational incentives are to protect users, it seems substantially more criticism will be required.

Google recently announced a plan to add interstitial warning pages before known-hostile sites, apparently sites with security exploits (Security Pro News 2006). But at least at present, Google focuses solely on the narrow problem of exploits – without regard for other kinds of harms.

## 9. Intervention under Existing Doctrines and Regulations

Seeing consumers harmed by malicious or deceptive search engine listings, policy-makers can attempt to improve outcomes. Policy makers could invoke certain existing rules and doctrines to that end.

For example, a longstanding policy propagated by the us Federal Trade Commission regulates advertisers' claims of ›free‹ products. The

FTC Guide Concerning Use of the Word ›Free‹ and Similar Representations requires that »such offers must be made with extreme care so as to avoid any possibility that consumers will be misled or deceived.« The FTC further requires that when ›free‹ offers carry conditions or obligations, all such terms »should be set forth clearly and conspicuously at the outset of the offer [...] in close conjunction with the offer of ›free‹ merchandise or service.« The FTC goes on to report that use of a footnote or asterisk is not sufficient to satisfy these disclosure obligations.

Widespread search engine ads fair poorly under this standard. Consider ads that appear in a standard Google search for »ringtones« (for additional examples, see EDELMAN 2006c):

»Unlimited free ringtones: 500,000 tones. Get them all free. No subscription required.«

»Free Ringtones: Download Free Ringtones. Easy! Don't Pay – Limited time – Hurry up«

»Ringtones: Get Free Ringtones Now. Supports All Phones and Carriers. 100% Free.«

»100% Free Ringtones: Download Ring Tones to Your Phone. 1000's to choose from – All Free!«

In fact, not one of the associated sites actually offers service plans that are free. Some offer free trials of limited duration, while others offer »free« bonuses associated with users' initial signups for paid services. The text quoted above captures the full contents of the respective offers; no adjacent text provides any further clarifications. While additional disclosures often appear later in the subscription process (e.g. in fine print after a user clicks on an ad), the FTC's »outset of the offer« requirement seems to nullify any disclosures provided only at that later stage. All in all, it is hard to reconcile these advertisers' practices with applicable FTC rules.

These and other ads also seem to border on consumer fraud, in that the ads repeatedly make statements not borne out by further scrutiny. One ad quoted above claims an offer is for a ›limited time‹ – but by all indications, that's false, in that the offer has remained unchanged for an extended period. Another ad promises ›no subscription required‹ – when in fact a subscription plan, with automatic recurring charges, is the only way to receive the specified service. By their prominence and their strong language, these statements are highly likely to be material to users' decision-making. Yet they're demonstrably false.

It therefore seems that the search engine advertisers at issue are ripe for regulatory pursuit – following existing caselaw as to consumer fraud and misleading use of the word ›free‹ (see e.g. *FTC v. Consumerinfo.com, Inc.*, d/b/a/ Experian Consumer Direct).

While existing obligations clearly speak to duties of advertisers as to the substance of their respective ads, it is less clear whether existing duties apply to ad publishers, acting in their capacity of redistributing third parties' ads. The applicable FTC policy is generally written in the passive voice. For example, the FTC instructs that »all such [free] offers must be made with extreme care«, without specifically stating whether the resulting duties apply only to advertisers (the originators of such offers) or also to advertising publishers (which could be required to decline impermissible offers). Meanwhile, the Lanham Act specifically contemplates injunctive relief against publishers for distributing false advertising (15 USC § 1114(2)), preventing publishers from continuing such distribution in the future. By negative implication, the Lanham Act also provides for money damages in those instances where a publisher is not an »innocent infringer« (e.g. where a publisher »recklessly disregard[s]« an ad's deficiencies).

But the US Communications Decency Act's § 230 (CDA) offers search engines (and other electronic publishers) a remarkable protection: That search engines, as providers of »interactive computer service«, may not be treated as the publisher of content that others provide through those services. It appears that this grant of immunity might trump even FTC rules otherwise specifically on point. The one relevant exception to CDA § 230 is § 230(e)(2), providing that CDA § 230 does not alter intellectual property law. Since the false advertising provisions at issue are codified within the Lanham Act, there is a colorable argument that these false advertising provisions are intellectual property law within the meaning of § 230(e)(2), hence not blocked by the main § 230 grant of immunity. But to date, no case has tested this legal theory.

## 10. Policy Changes and Regulatory Interventions

But for the CDA §230 defense, search engines might also face liability under a general theory of negligence. If a search engine shows a listing (especially a paid listing, i.e. an ad) that causes harm to a user, and if the

search engine knew or reasonably should have known of the likely harm resulting from that listing, there are strong arguments for holding the search engine accountable for that harm. The party that most directly caused the harm is probably difficult or impossible to locate, and that party may well be judgment-proof relative to the amount of harm caused. Many such parties are similarly situated. If search engines are permitted to show such ads without regard for their consequences, users will suffer harm from a stream of unaccountable bad actors – even as search engines profit from each user clicking through to another dubious ad. Improved protections for consumers will only result if search engines are forced to intervene.

Increased duties on search engines match existing policies in other media. For example, the New York Times maintains a voluminous (4,500+ word) set of advertising policies, specifically requiring compliance with various FTC guidelines to prevent consumer deception. Google admittedly has far more advertisers than the New York Times, but Google's revenues are larger. Furthermore, Google already reviews ads for compliance with other requirements (e.g. the Google Editorial Guidelines), blunting any argument that review is impossible or impractical. Furthermore, many of the problematic ads could readily be identified using simple keyword searches (e.g. >free<), making such review particularly efficient.

Finally, policy might grant enforcement capability to private parties, so as to minimize the burden on government agencies. A prominent technology lawyer is already publicly evaluating claims against search engines arising out of their linking to illegal online gambling. (See *Rothken Law Firm 2006*: »If the following facts are true please click here to possibly participate in a current case: You lost money at internet gambling after clicking on sponsored net gambling ads on one or more major search sites and you were a California resident at the time.«) But consumers' rights need not be limited to gambling losses. Whether by statute or through precedent, private attorneys could readily vindicate other harms consumers suffer as a result of search engines' ads.

An alternative regime would require search engines to investigate or take action under a notice-and-takedown theory. Those who identify improper ads could report them via some designated mechanism, at which point the search engine would notify the advertiser of the complaint. The flagged ad would then be removed if the advertiser could not provide a satisfactory rebuttal within a specified period (see e.g. the *Digi-*

tal Millennium Copyright Act (DMCA) notice and takedown procedure, 17 § 512(c)).

The core policy question – and possible policy change – remains whether a search engine ought to be responsible for the ads it is paid to show. The CDA § 230 grants immunity rings true where a web site simply distributes user-submitted comments with nothing more, e.g. a standard free online discussion site. But where a search engine is *paid* to show ads, and exercises considerable discretion in what ads to approve (e.g. via various rules of its own creation), it is puzzling to see the search engine escape rules that apply equally to other media. Even if search engines find editorial approval difficult due to their near-instantaneous publication and their large number of advertisers, search engines could still be required to take action when particular improper ads are specifically brought to their attention. Nonetheless, CDA § 230 seems to establish precisely the contrary result, i.e. that a search engine need not take any such action, no matter the content of an ad and no matter the notice a search engine receives. This policy flies in the decision of an overarching goal of treating electronic media similarly to print media (see e.g. President's Working Group on Unlawful Conduct on the Internet 2000). This policy decision also faces considerable criticism for the possibility that it would allow web sites to distribute, e.g., racially discriminatory housing ads widely prohibited in other media (VOLOKH 2006). The statute may equally bear revisiting in the context of search engine advertising.

## 11. Conclusions

Users and researchers don't control what sites do, nor can they control search engines' policies. Even security companies can't fully address the situation. Robust client-side security protects against exploits, but it generally cannot defend users against scams, nor against programs users *decide* to install (even if after misleading or deceptive installation solicitations). Users can protect themselves somewhat through increased information and investigation, including the research provided by SiteAdvisor. But such efforts only directly help those users who take the time and make the effort to get informed.

The scope of these problems is alarming – so many ways, so prominent and so easy to find, by which top search engines lead users to sites

that turn out to be untrustworthy or worse. But the online pharmacy example offers reason for considerable optimism: There, search engines saw a problem, designed a solution, and implemented it in a way that offers users real protection. Could similar solutions emerge to protect users from spyware, spam, and other Internet plights?

It seems there are plenty of sites search engines could properly remove from their listings and from their ad networks. A Utopian Internet would probably be spyware-free and spam-protected, and it would have no place for sites that try to charge users for software that's actually free. Exploit sites are even more noxious – so the case for their removal from search engines seems particularly strong. Such improvements would require considerable effort by search engines, but these improvements could offer competitive advantage to a search engine attempting to distinguish itself from rivals.

Meanwhile, there's a real problem out there – tens of thousands of sites that, in SiteAdvisor's analysis, pose serious risks of harming users. Navigating the Web via a search engine won't prevent users from stumbling onto one of these sites, and search results provide users with little indication of site safety. Users can exert some control by choosing one search engine over another or by choosing organic results instead of sponsored results, but users still need more information. Otherwise, it's only a matter of time before users end up on dangerous sites, where just one bad click can produce harmful consequences.

## References

- Communications Decency Act*. 47 USC § 230. Online: [http://www4.law.cornell.edu/uscode/html/uscode47/usc\\_sec\\_47\\_00000230----000-.html](http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html)
- ComputerWorld: Analysis: Paid Search Results Often Not Worth the Click*. Online: <http://www.computerworld.com/printthis/2006/0,4814,108416,00.html>. 2006
- Consumer Reports: A Matter of Trust: What Users Want from Web Sites*. Online: <http://www.consumerwebwatch.org/pdfs/a-matter-of-trust.pdf>. 2002
- Digital Millennium Copyright Act*. 17 USC § 512(c). Online: [http://www4.law.cornell.edu/uscode/html/uscode17/usc\\_sec\\_17\\_00000512----000-.html](http://www4.law.cornell.edu/uscode/html/uscode17/usc_sec_17_00000512----000-.html)
- EDELMAN, B.: *Pushing Spyware through Search*. Online: <http://www.benedelman.org/news/012606-1.html>. 2006a

- EDELMAN, B.: *Search Engine Safety, Revisited*. Online: <http://www.benedelman.org/news/051206-1.html>. 2006b
- EDELMAN, B.: *False and Deceptive Pay-Per-Click Ads*. Online: <http://www.benedelman.org/ppc-scams/>. 2006c
- EDELMAN, B.; H. ROSENBAUM: *The Safety of Internet Search Engines*. Online: [http://www.siteadvisor.com/studies/search\\_safety\\_may2006.html](http://www.siteadvisor.com/studies/search_safety_may2006.html). 2006
- FTC *Guide Concerning Use of the Word »Free« and Similar Representations*. Online: <http://www.ftc.gov/bcp/guides/free.htm>
- FTC v. *Consumerinfo.com, Inc., d/b/a/Experian Consumer Direct*. Online: <http://www.ftc.gov/os/caselist/0223263/0223263.htm>
- Google *Editorial Guidelines*. Online: <https://adwords.google.com/select/guidelines.html>
- Google *Zeitgeist*. Online: <http://www.google.com/press/zeitgeist.html>
- Google's *Online Pharmacy Qualification Process*. Online: [http://www.google.com/adwords/pharmacy\\_qualification.html](http://www.google.com/adwords/pharmacy_qualification.html)
- I PROSPECT: *Search Engine User Behavior Study*. Online: [http://www.iprospect.com/premiumPDFs/WhitePaper\\_2006\\_SearchEngineUserBehavior.pdf](http://www.iprospect.com/premiumPDFs/WhitePaper_2006_SearchEngineUserBehavior.pdf). 2006
- New York Times Advertising Terms & Conditions / Advertising Acceptability Guidelines*. Online: <https://placead.nytimes.com/terms.htm>
- NIelsen NETRATINGS: *Online Search Hits All-Time High of 5.7 Billion Searches*. Online: [http://www.nielsen-netratings.com/pr/pr\\_060302.pdf](http://www.nielsen-netratings.com/pr/pr_060302.pdf). 2006
- PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET: *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*. Online: <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>. 2000
- Rothken Law Firm: *Internet Gambling Losses*. Online: <http://www.techfirm.com>. 2006
- Search Engine Mega-List*. Online: <http://www.search-engines-megalist.com/>
- Security Pro News: *Google Warning Users About Badware Links*. Online: <http://www.securitypronews.com/insiderreports/insider/spn-49-20060804GoogleWarningUsersAboutBadwareLinks.html>. 2006
- SiteAdvisor: *Not So Practical Web Safety Advice*. Online: [http://blog.siteadvisor.com/2006/01/notsopractical\\_web\\_security\\_ad.shtml](http://blog.siteadvisor.com/2006/01/notsopractical_web_security_ad.shtml). 2006
- SiteAdvisor *FAQ*. Online: <http://www.siteadvisor.com/press/faqs.html>. 2006
- TECHTARGET: *End User's Spyware Prevention Checklist*. Online: [http://searchsecurity.techtargert.com/tip/1,289483,sid14\\_gci1124220,00.html](http://searchsecurity.techtargert.com/tip/1,289483,sid14_gci1124220,00.html). 2005

VOLOKH, E.: *Lawsuit Against Craigslist*. Online: <http://volokh.com/posts/1139594512.shtml>. 2006

Yahoo!: *Top Searches*. Online: <http://tools.search.yahoo.com/top2005/>. 2005

*Yahoo Sponsored Search Listing Guidelines*. Online: <http://searchmarketing.yahoo.com/rc/srch/relevancy.php>