http://www.cnn.com/2006/TECH/internet/11/15/internet.blocking.ap/index.html

Government study: Web 1 percent porn

POSTED: 10:22 a.m. EST, November 16, 2006

PHILADELPHIA, Pennsylvania (AP) -- About 1 percent of Web sites indexed by Google and Microsoft are sexually explicit, according to a U.S. government-commissioned study.

Government lawyers introduced the study in court this month as the Justice Department seeks to revive the **1998 Child Online Protection Act**, which required commercial Web sites to collect a credit card number or other proof of age before allowing Internet users to view material deemed "harmful to minors."

The U.S. Supreme Court blocked the law in 2004, ruling it also would cramp the free speech rights of adults to see and buy what they want on the Internet. The court said technology such as **filtering software** may work better than such laws.

The American Civil Liberties Union -- which challenged the law on behalf of a broad range of Web publishers -- said the study supports its argument that filters work well.

The study concludes that the strictest filter tested -- AOL's Mature Teen -- blocked 91 percent of the sexually explicit Web sites in indexes maintained by Google Inc. and Microsoft Corp.'s MSN.

Filters with less restrictive settings blocked at least 40 percent of sexually explicit sites according to the study of random Web sites by Philip B. Stark, a statistics professor at University of California, Berkeley.

"Filters are more than 90 percent effective, according to Stark," ACLU attorney Chris Hansen said Tuesday during a break in the trial. "Also with filters, it's up to the parents how to use it, whereas COPA requires a one-solution-fits-all (approach)."

COPA follows Congress' unsuccessful 1996 effort to ban online pornography. The Supreme Court in 1997 deemed key portions of that law unconstitutional because it was too vague and trampled on adults' rights. It would have criminalized putting adult-oriented material online where children can find it.

The 1998 law narrowed the restrictions to commercial Web sites and defined indecency more specifically.

In 2000, Congress also passed a law requiring schools and libraries to block porn using software filters if they receive certain federal funds. The high court upheld that law in 2003.

Justice Department lawyers Theodore Hirt and Raphael Gomez declined to comment Tuesday on Stark's findings.

Stark prepared the report based on information the Justice Department obtained through subpoenas sent to search engine companies and Internet service providers.

Google refused one such subpoena for 1 million sample queries and 1 million Web addresses in its database, citing trade secrets. A judge limited the amount of information the company had to provide.

Stark also examined a random sample of search-engine queries. He estimated that 1.7 percent of search results at Time Warner Inc.'s AOL, MSN, and Yahoo Inc. are sexually explicit and 1.1 percent of Web sites cataloged at Google and MSN fall in that category.

About 6 percent of searches yield at least one explicit Web site, he said, and the most popular queries return a sexually explicit site nearly 40 percent of the time.

But filters blocked 87 percent to 98 percent of the explicit results from the most popular searches on the Web, Stark found.

Stark also said that about half the sexually explicit Web sites found in the Google and MSN indexes are foreign, making them beyond the reach of U.S. law. But he agreed with government assertions that the most popular sites are domestic.

"COPA -- right out of the bat -- doesn't block the 50 percent (posted) overseas," Hansen said. "So COPA is substantially less than 50 percent effective."

Closing arguments in the 4-week, non-jury trial before Senior U.S. District Judge Lowell Reed Jr. are expected Monday.

The law -- signed by then-President Clinton -- requires Web sites to get credit card information or some other proof of age from adults who want to view material that may be considered harmful to children. It would impose a $50,000 fine and 6-month prison term on commercial Web site operators that allow minors to view such content, which is to be defined by "contemporary community standards."

The law has yet to be enforced. The U.S. Supreme Court upheld a preliminary injunction, ruling in June 2004 that the plaintiffs were likely to prevail.

The plaintiffs -- including Salon.com -- say they would fear prosecution under the law for publishing material as varied as erotic literature to photos of naked inmates at Iraq's Abu Ghraib prison.

Copyright 2006 The Associated Press. All rights reserved.

http://www.msnbc.msn.com/id/17736176/

Judge throws out Internet blocking law

Ruling states parents must protect children through less restrictive means

By Maryclaire Dale, Associated Press

Updated: 32 minutes ago, March 22, 2007

PHILADELPHIA - A federal judge on Thursday threw out a 1998 law that makes it a crime for commercial Web site operators to let children access "harmful" material.

In the ruling, the judge said parents can protect their children through software filters and other less restrictive means that do not limit the rights of adults to free speech.

"Perhaps we do the minors of this country harm if First Amendment protections -- which they will with age inherit fully -- are chipped away in the name of their protection," wrote Senior U.S. District Judge Lowell Reed Jr. who presided over a 4-week trial last fall.

The law would have criminalized Web sites that allow children to access material deemed "harmful to minors" by "contemporary community standards". The sites would have been expected to require a credit card number or other proof of age. Penalties included a $50,000 fine and up to 6 months in prison.

Sexual health sites, the online magazine Salon.com, and other Web sites backed by the American Civil Liberties Union challenged the law. They argued that the Child Online Protection Act was unconstitutionally vague and would have had a chilling effect on speech.

The U.S. Supreme Court upheld a temporary injunction in 2004 on grounds the law was likely to be struck down and was perhaps outdated.

Technology experts said parents now have more serious concerns than Web sites with pornography. For instance, the threat of online predators has caused worries among parents whose children use social-networking sites such as News Corp.'s MySpace.

The case sparked a legal firestorm last year when Google challenged a Justice Department subpoena seeking information on what people search for online. Government lawyers had asked Google to turn over 1 million random Web addresses and a week's worth of Google search queries.

A judge sharply limited the scope of the subpoena which Google had fought on trade secret, not privacy, grounds.

- *Lawyers argue validity of '98 online law* (*http://www.msnbc.msn.com/id/15821117/*)
- *Software helps hunt down child porn online* (*http://www.msnbc.msn.com/id/7425082/*)
- *Dateline: Staying ahead of 'predators'* (*http://www.msnbc.msn.com/id/15157979/*)

http://www.msnbc.msn.com/id/17708550/

Privacy for Internet names moves forward

Proposal that would give more options to small businesses, individuals

By Anick Jesdanun

Updated: 4:57 p.m. ET March 20, 2007

NEW YORK - Many owners of Internet addresses face this quandary: Provide your real contact information when you register a domain name and subject yourself to junk or harassment. Or enter fake data and risk losing it outright.

Help may be on the way as a key task force last week endorsed a proposal that would give more privacy options to small businesses, individuals with personal Web sites, and other domain name owners.

"At the end of the day, they are not going to have personal contact information on public display," said Ross Rader, a task force member and director of retail services for registration company Tucows Inc. "That's the big change for domain name owners."

At issue is a publicly available database known as **Whois**. With it, anyone can find out the full names, organizations, postal and e-mail addresses and phone numbers behind domain names.

Hearings on the changes are expected next week in Lisbon, Portugal before the Internet Corporation for Assigned Names and Numbers -- or ICANN -- the main oversight agency for Internet addresses.

Resolution, however, could take several more months or even years with crucial details on implementation still unsettled and a vocal minority backing an alternative.

Under the endorsed proposal -- some 6 years in the making -- domain name registrants would be able to list third-party contact information in place of their own to the chagrin of businesses and intellectual-property lawyers worried that cybersquatters and scam artists could more easily hide their identities.

"It would just make it that much more difficult and costly to find out who's behind a name," said Miriam Karlin, manager of legal affairs for International Data Group Inc., publisher of *PC World* and other magazines. She said she looks up Whois data daily to pursue trademark and copyright violators.

Privacy wasn't a big consideration when the current addressing system started in the 1980s. Back then, government and university researchers who dominated the Internet knew one another and didn't mind sharing personal details to resolve technical problems.

Today, the Whois database is used for much more. Law-enforcement officials and Internet service providers use it to fight fraud and hacking. Lawyers depend on it to chase trademark and copyright violators. Journalists rely on it to reach Web site owners. And spammers mine it to send junk mailings for Web site hosting and other services.

And Internet users have come to expect more privacy and even anonymity. Small businesses work out of homes. Individuals use Web sites to criticize large corporations or government officials. For many, the Whois database reveals too much.

The requirements for domain name owners to provide such details also contradict -- in some cases -- European privacy laws that are stricter than those in the United States.

Registration companies generally don't check contact information for accuracy. But submitting fake data could result in missing important service and renewal notices. It also could be grounds for terminating a domain name.

Over the past few years, some companies have been offering proxy services for a fee, letting domain name owners list the proxy rather than themselves as the contact.

It's akin to an unlisted phone number, though with questionable legal status. The U.S. Government has banned proxies entirely for addresses ending in ".us" even after many had already registered names behind them.

Critics also complain that such services can be too quick or too slow -- depending on whom you ask -- in revealing identities under legal pressure.

"Right now there's no regulation, no accreditation, no standards," said Margie Milam, general counsel for MarkMonitor, a brand-protection firm. "Some can take weeks which can slow down investigations."

The task force proposal -- known as operational point of contact -- would make third-party contacts a standard offering. Domain name owners could list themselves, a lawyer, a service provider, or just about anyone else. That contact would forward important communications back to the owner.

Details must still be worked out. But the domain name registrant rather than the proxy would likely be clearly identified as the legal owner unlike the current, vague arrangement. ICANN's staff also pressed for more clarity on to whom and under what circumstances the outside contact would have to release data.

Although that proposal received a slight majority on the Whois task force, some stakeholders including businesses and lawyers have pushed an alternative known as special circumstances. Domain name holders would have to make personal contact details available -- as they do today -- unless they can justify a special circumstance such as running a shelter for battered women.

"On the whole, society is much better off having this kind of transparency and accountability," said Steven Metalitz, an intellectual-property lawyer on the task force.

ICANN's Council of the Generic Names Supporting Organization plans public hearings in Lisbon, after which it could make a recommendation or convene another task force to tackle implementation details.

Supporters of the new proposal remain hopeful that resolution is near.

"A lot of public interest groups have been waiting a long time to see if this process actually works or if it's just a charade," said Wendy Seltzer, a non-voting task force member and fellow with Harvard University's Berkman Center for Internet and Society. "If this turns out to have been for naught, you will have a lot of frustrated people."