# [***Internet users find barriers to sites at school, work, library;***](https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:47KF-21G0-01JV-C0NB-00000-00&context=1516831) [***Governments, firms, universities and ISPs put up fences. Some do it by design. Others, however, do it unintentionally.***](https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:47KF-21G0-01JV-C0NB-00000-00&context=1516831)

Philadelphia Inquirer

January 2, 2003 Thursday CITY-D-EAST EDITION

Copyright 2003 Philadelphia Newspapers, LLC  All Rights Reserved



**Length:** 1062 words

**Byline:** By Anick Jesdanun; Associated Press

**Body**

On the Internet, you can learn about virtually anything. You can seek comfort from others similarly afflicted by a rare disease, or explore such sensitive topics as birth control.

Just as long as you are not connecting from work, a school or a public library, that is.

And if you are using any number of e-mail services that employ junk-mail filters - or a search engine such as Google - do not count on wholly unfettered access, either.

As the Internet matures, governments, corporations, universities and service providers are erecting fences, some by design, others often unintentionally.

Stop signs, detours, road closures and guarded gateways to exclusive communities went up in 2002 as never before.

Jonathan Zittrain, a Harvard University law professor who specializes in the Internet, said he worries that little public discussion attends the construction of these impediments to the free flow of information.

"We could end up with an increasing amount of filtering in the middle without anyone particularly raising much of a hue and cry about what impact it has," Zittrain said.

Knowledge and innovation are at risk if publishers and researchers must get permission to pass through each gateway, Fred von Lohmann, an attorney for the Electronic Frontier Foundation in San Francisco, argues.

Consider the World Wide Web.

When Tim Berners-Lee designed it in 1990, security firewalls did not exist. He did not have to ask anyone to open up the software communications port used for Web traffic. Today, given the increased risks of viruses and hacking, firewalls seal off unused ports, forcing developers of new services to invent workarounds.

Despite extensive technical adjustments, 1 in 5 firewalls continues to pose problems for Net2Phone, which provides cheap long-distance calls over the Internet. And some companies intentionally block PalTalk, an instant-messaging service with audio and video.

Other technical obstacles, such as a technique that hides several computers behind a single Internet address, are becoming more common, disrupting online games and other emerging services that need unique addresses, said Fred Baker, chairman of the Internet Society, an organization of Internet architects and professionals.

"It becomes much more difficult nowadays to deploy a new application," Baker said. "It's a very legitimate question whether we would have the Web today if we had firewalls 10 years ago."

Of greater concern to some are fences erected to impose social values.

The Internet worked well when intermediary computers did no more than their assigned role of passing data packets along to the next computer closer to the destination, Danny Weitzner of the standards-setting World Wide Web Consortium said.

Now those computers, controlled by a multitude of parties, are being increasingly called upon to make social judgments: Is that packet a part of an advertisement, pornography or terrorist communication?

Sex education sites, resources on gun control, and online bookstores can get sidelined by mistake or by some policy decision outside the recipient's control.

Totalitarian regimes such as China's impose national filters, but even the United States employs such controls. U.S. public schools are required by a disputed law to block pornography if they are to receive federal Internet funding, while many public libraries and companies do it on their own.

"As the Internet has become profitable and boundaries of the Internet expanded, the seamier side and the potential traps have expanded accordingly," said Frank Gillman, director of technology at Allen Matkins, a Los Angeles law firm that employs filtering controls.

In the last year, Pennsylvania passed a law requiring Internet service providers to block child-pornography sites at the request of prosecutors, giving them powers once limited to the courts. The state Attorney General's Office so far has asked 17 service providers to block 340 sites.

The recording industry also briefly tried to compel four service providers to block a Chinese Web site accused of distributing pirated music. It later dropped that lawsuit.

Panama's government tried to block Internet-based phone calls, but its Supreme Court later struck down the effort.

Meanwhile, the Church of Scientology International used copyright laws to pressure Google to remove listings for a Norwegian site run by critics. The French and German governments cited their laws in getting the search engine to remove hate sites.

"The Internet is not the Wild West, and laws that exist in other media or other forms don't disappear," said Dave Baker, vice president of law and public policy at EarthLink, a nationwide Internet service provider.

These fences are not always avoidable, their defenders say.

Without content filtering in the workplace, employers lose productivity and risk lawsuits if workers access pirated or sexually oriented material, said Harold Kester, chief technology officer at Websense, a maker of filtering software.

Likewise, without firewalls, security threats increase, rendering the Internet unusable.

The same goes for bandwidth-management tools such as Palisade Systems' PacketHound, which lets networks control how much traffic is permitted for high-volume services such as sharing movies and music.

"When you have certain threats, you give up certain rights to protect against those threats," Stephen Brown, Palisade's product marketing manager, said.

Some high-speed service providers also employ bandwidth controls aimed at file-sharing systems. Time Warner Cable, for instance, has blocked some users who share large numbers of files and thus degrade the network for others.

Notwithstanding the concerns over piracy of copyright materials, when universities restrict file-sharing, students can lose access to hard-to-find documentaries and other material.

The fight against junk e-mail also sometimes backfires. Legitimate mail such as newsletters for support groups sometimes gets mistakenly blocked, often without senders or recipients even knowing.

Other barriers are possibly on the way, particularly as wireless access proliferates in the coming year. Will the open roads promised by WiFi dominate, or the gated communities favored by ***cell-phone*** providers?

"Those battles are just starting to be waged," Zittrain, the Harvard law professor, said. "They could greatly determine just how innovating one can be in that space."

**Load-Date:** January 2, 2003

**End of Document**