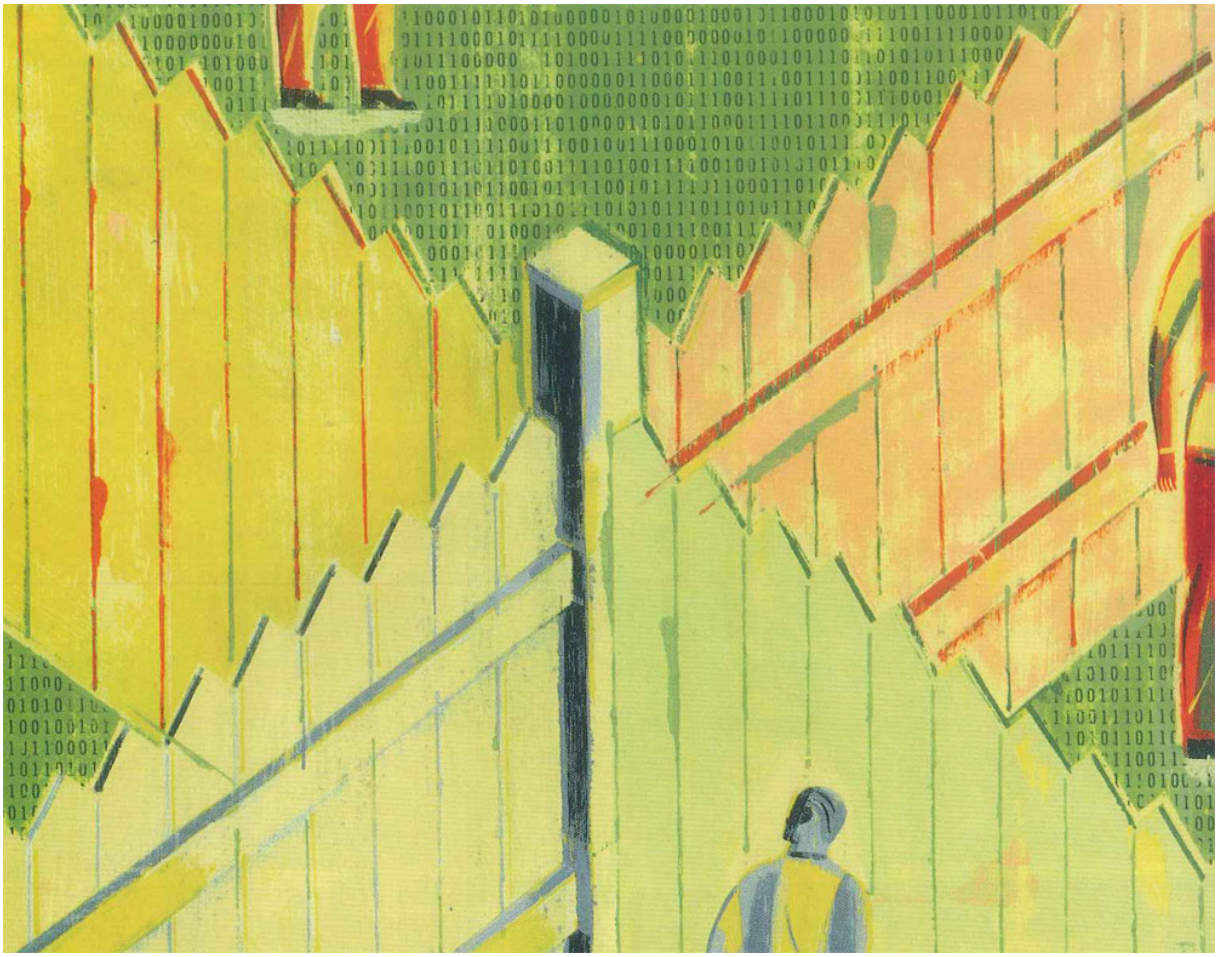
Science & Technology

When the Net Becomes a Wall

State control, market forces, and the Internet’s power to divide.

By
David J. Craig
|
Fall 2006



Brad Yeo

Conventional wisdom says that the Internet is an unstoppable democratic force. That in cyberspace, start-ups always get a fair crack at the fat cats, bloggers eventually take down the tyrants, and free speech is inviolable.

The problem with that notion is it assumes tha big business and government regulators can’t fully exert their power on the network. How can companies maintain market dominance, the thinking goes, when new competitors are keystrokes away? How can dictators effectively censor information when tech-savvy dissidents are one step ahead.

In fact, Columbia experts say, the Internet today is not so much transforming societies as it is mirroring political cultures. As evidence they point to two current trends — the increasing deftness with which some nations, especially China, control what is available online, and the push in the United States to give big business more influence over which Web sites you view.

“People have always said that the Internet is bound to sweep away established businesses and political and cultural restrictions,” says Eli Noam, a professor of finance and economics director of the Institute for Tele-Information at Columbia Business School. “That libertarian dream is falling by the wayside, with the encroachment of market forces and state control. The Internet isn’t the Wild West anymore. It’s being domesticated.”

Pricey pipes

It’s easy for Americans to think of the Internet as an open playing field, because our laws encourage and enable bold business innovation and the free exchange of ideas online. US courts, for instance, have periodically turned a blind eye to copyright violation in order to let promising technologies develop — as they did initially with music-downloading programs — and they’ve repeatedly struck down anti-pornography laws for fear of chilling artistic and other expression.

But another fundamental principle that shapes our Internet is under attack from corporate America, according to Tim Wu, a Columbia law professor who teaches courses on technology, telecommunications, copyright, and international trade issues. Last year, the Federal Communications Commission dropped its so-called “network neutrality” provision requiring Internet service providers (ISPs) to treat all Web content equally.

That law forced phone and cable companies to deliver the Drudge Report to your computer with the same signal quality as CNN.com. It also prohibited ISPs from

blocking any Web sites outright, Wu says. Now, news reports say service providers are planning to sell Web-content producers such as Amazon, Microsoft, or *The New York Times* passage on a new Internet “fast lane,” while nonpaying Web sites will be relegated to the slower part of the wires. How slow? No one knows, but the ISPs get to decide, and it will be slower than the latest technology allows. The ISPs say they need the extra cash to continue improving broadband capabilities, especially to accommodate online video.

Wu has emerged as a leading proponent of an effort by public advocacy groups to convince Congress to add network neutrality language to major telecommunications legislation now being considered by the US Senate. The 34-year-old cyberlaw expert testified before a US House committee on the matter this spring, arguing that the Internet is as essential to our economy as are the highways and the electric grid, and that all Americans should have the same basic rights to it. (The House voted against neutrality provisions in May, and as of *Columbia*’s September 8 printing, the Senate had not yet voted on a bill sponsored by Alaska Republican Ted Stevens that had no neutrality provisions.) The e-commerce markets now operating on the Internet “are in many ways an economist’s dream,” Wu told the House committee. “Start-up costs are minimal.

Many successful businesses began with just an idea and a good Web site. . . . But this thriving market has an Achilles heel, for there’s one part of the Internet that isn’t competitive: broadband access.”

As long as the vast majority of Americans have no more than two choices for broadband access, Wu says, the phone and cable companies have too much leverage over Web-content producers. He worries that if a new fastlane is offered on the Internet, ISPs will have incentive to not upgrade the Internet’s slow lane. In order to extract fast lane payments from deep-pocketed content providers, in other words, they could intentionally diminish the service available to all others. “The potential for abuse of market power is obvious,” Wu says. “These fast-lane tolls could be likened to radio payola, where getting radio play is no longer about recording the best song, but about cutting the best deal,” he says. “That hurts diversity, quality, and innovation.”

Eventually, “we’re going to see less folk culture flourishing online and a slower stream of innovative companies,” says Wu, coauthor of the recent book, *Who Controls the Internet?* “New companies will begin as ‘partners’ with our cable or

phone companies, which is very different from how Google, Netflix, or YouTube started."

Eli Noam, who served as New York State public-service commissioner in the early 1990s, agrees that the deregulation of service providers will sap vitality from the Internet. But he thinks the ISPs' price discrimination among Web sites is inevitable; he actually predicted it in a 1994 paper. Although many large Internet companies like Yahoo! and Google support network neutrality, he says, "there are lots of banks and broadcasters and corporations that want a special quality assurance on the Internet and are willing to pay for it, so how do you stop these willing sellers and buyers from coming together?"

In an August 29 *Financial Times* column, Noam proposed a compromise on network neutrality: Deregulate only that deep section of the Internet known as the backbone, which interconnects the "last-mile" networks owned by ISPs that deliver service to the end user. More competition exists between companies that own parts of the backbone, Noam says, than between last-mile ISPs. He says that ISPs also should have to deliver all content. The service providers have promised that they won't block any Web content or applications, but several tried back when it was illegal; the North Carolina phone company Madison River, for instance, in 2004 blocked their DSL customers from using a voice-over-Internet protocol (VoIP) service until the FCC intervened. "What happens if a particular community boycotts a service provider for carrying porn or pro-life Web sites?" Noam asks. "Network neutrality always offered the service providers political protection against those pressures."

The Great Firewall

While in Beijing this summer researching a new book, Wu was chagrined to realize how much he relies on Wikipedia. It's off-limits in China, blocked by the firewall that screens foreign Web pages for content inconsistent with state ideology. So was the BBC most days. Wu could usually read *The New York Times*, minus any stories critical of China. Like all foreign sites, though, the *Times* came up slowly because the available bandwidth moving across China's border is small compared to that within the country. Wu did manage to do research online, accessing the Web sites of libraries and many publications from the West. And if he really wanted to read an uncensored report — even on hot-button topics that are supposed to trip the filter,

like Falun Gong, Tibet, democracy, or human rights — he could often locate it after surfing around on English-language sites for a while.

That China's filtering system isn't impenetrable has led many Western critics of Web culture to conclude that the nation's increasingly elaborate efforts to harness the Internet are futile. They say that although every blog is monitored and self-censoring search engines like one provided by Google this year complement China's firewall, the most freethinking among China's 111 million Web surfers will still access unapproved sites and connect to like-minded citizens. "China's new Cultural Revolution will be driven this time from the bottom up," Thomas L. Friedman wrote in a *Times* column last fall, "by podcasters with Apple's little white iPods."

That's the wrong way to look at it, according to Wu. "Yes, there will always be techno-geeks with the determination to set up secret portals outside of China, so people who know about it can get around the filter," he says. "But how many people are going to risk doing that? It's always going to be the underground, and as soon as any avoidance strategy reaches a critical mass, the government will put its foot down. . . . China is being very smart about not pushing to control every aspect of the Internet, about allowing people to feel a certain sense of freedom."

And China's control strategies so far are keeping pace with new technology, Wu says, effectively limiting "how much freedom most people experience. Some of that control is based on self-censorship, because the fear of being arrested for writing the wrong thing online is palpable. . . . China is creating a new type of network, one that's pulling away from the Internet in the West and balancing the needs of a closed government and an open economy."

Perhaps, then, the most important question regarding the Internet today isn't how it's affecting other countries, but vice versa. Wu and Noam both predict that the US may face a struggle in the next decade to preserve its open network model as the world standard, as Americans represent an ever-smaller percentage of Internet users. China, which today has almost as many Internet users as the United States, is trying to influence global protocols for Wi-Fi broadband, for instance, by proposing that all computers used within its borders be required to contain a device that automatically registers its owner with a central identification point. South Korea and European nations, meanwhile, are adopting strict government licensing requirements for the emerging application of on-demand Internet TV. Regulating over-the-air broadcast television made sense, Noam says, because there are only a

few frequencies available, but no such technological rationale exists online. “[I]f the future of all media is on broadband,” he wrote in *The Financial Times* last fall, it will be “one of state licensing and controls.”

It’s easy to forget that the Internet, hardly incorruptible, consists of cables, wires, and routers whose owners are easily influenced by the lure of profit and the rule of law. While Google and Yahoo! have earned special enmity for doctoring their products for use in China, Wu says, in the past five years nations increasingly have been getting their way in cyberspace by playing hardball: The Wall Street Journal online now abides by Australia’s strict libel laws after being dragged into court there, Yahoo! removed from its auctions Nazi memorabilia after being sued in France to comply with laws there banning the trafficking of the items, and the US shut down overseas online gambling operations by threatening legal actions against credit-card companies that accepted the charges. European countries force their ISPs to screen out pornographic and illegal adoption sites, moreover, while Saudi Arabia’s firewall blocks Web sites that promote drug use and Muslim-Christian dialogue.

“We’ve lived with the Internet long enough now to take it for granted, but it’s changing fast, and a good outcome is not guaranteed,” says Wu. “What’s going to happen next is Web issues are going to become some of the most important international trade and policy issues. How is the US going to deal with Russia and other countries that don’t enforce copyrights for music and video downloading? Will we see an Internet version of the Cold War with our network ideology and China’s growing further apart? America’s open model is still the default for other countries right now, but they’re shaping it for themselves, chipping away.”

Read more from ***David J. Craig***



Guide to school abbreviations

All categories >
Read more from ***David J. Craig***