A Net of Control

UNTHINKABLE: How the Internet could become a tool of corporate and government power, based on updates now in the works

By Steven Levy
NEWSWEEK INTERNATIONAL

Issues 2004 — Picture, if you will, an information infrastructure that encourages censorship, surveillance and suppression of the creative impulse. Where anonymity is outlawed and every penny spent is accounted for. Where the powers that be can smother subversive (or economically competitive) ideas in the cradle, and no one can publish even a laundry list without the imprimatur of Big Brother. Some prognosticators are saying that such a construct is nearly inevitable. And this infrastructure is none other than the former paradise of rebels and free-speechers: the Internet.
TO THOSE EXPOSED to the Panglossian euphoria of Net enthusiasts during the 1990s, this vision seems unbelievable. After all, wasn’t the Internet supposed to be the defining example of empowering technology? Freedom was allegedly built into the very bones of the Internet, designed to withstand nuclear blasts and dictatorial attempts at control. While this cyberslack has its downside—porn, credit-card fraud and insincere bids on eBay—it was considered a small price to pay for free speech and friction-free business models. The freedom genie was out, and no one could put it back into the bottle.

Certainly John Walker believed all that. The hackerish founder of the software firm Autodesk, now retired to Switzerland to work on personal projects of his choosing, enjoyed “unbounded optimism” that the Net would not only offset the
powers of industry and government but actually restore some previously threatened personal liberties. But in — the past couple of years, he noticed a disturbing trend. Developments in technology, law and commerce seemed to be directed toward actually changing the open nature of the Net. And Internet Revisited would create opportunities for business and government to control and monitor cyberspace.

In September Walker posted his fears in a 28,000-word Web document called the Digital Imprimatur. The name refers to his belief that it’s possible that nothing would be allowed to even appear on the Internet without having a proper technical authorization.

How could the freedom genie be shoved back into the bottle? Basically, it’s part of a huge effort to transform the Net from an arena where anyone can anonymously participate to a sign-in affair where tamperproof “digital certificates” identify who you are. The advantages of such a system are clear: it would eliminate identity theft and enable small, secure electronic “microtransactions,” long a dream of Internet commerce pioneers. (Another bonus: arrivederci, unwelcome spam.) A concurrent step would be the adoption of “trusted computing,” a system by which not only people but computer programs would be stamped with identifying marks. Those would link with certificates that determine whether programs are uncorrupted and cleared to run on your computer.

The best-known implementation of this scheme is the work in progress at Microsoft known as Next
Generation Secure Computing Base (formerly called Palladium). It will be part of Longhorn, the next big Windows version, out in 2006. Intel and AMD are onboard to create special secure chips that would make all computers sold after that point secure. No more viruses! And the addition of "digital rights management" to movies, music and even documents created by individuals (such protections are already built into the recently released version of Microsoft Office) would use the secure system to make sure that no one can access or, potentially, even post anything without permission.

The giants of Internet commerce are eager to see this happen. "The social, economic and legal priorities are going to force the Internet toward security," says Stratton Sclavos, CEO of VeriSign, a company built to provide digital certificates (it also owns Network Solutions, the exclusive handler of the "dot-com" part of the Internet domain-name system). "It’s not going to be all right not to know who’s on the other end of the wire." Governments will be able to tax e-commerce—and dictators can keep track of who’s saying what.

Walker isn’t the first to warn of this ominous power shift. The Internet’s pre-eminent dean of darkness is Lawrence Lessig, the Stanford University guru of cyberlaw. Beginning with his 1999 book "Code and Other Laws of Cyberspace," Lessig has been predicting that corporate and regulatory pressures would usurp the open nature of the Net, and now says that he has little reason to retract his pessimism. Lessig understands that restrictive copyright and Homeland Security laws give a legal rationale to "total control," and also knows that it will be sold to the people as a great way to stop thieves, pirates, malicious hackers, spammers and child pornographers. "To say we need total freedom isn’t going to win," Lessig says. He is working hard to promote alternatives in which the law can be enforced outside the actual architecture of the system itself but admits that he considers his own efforts somewhat quixotic.

Does this mean that John Walker’s nightmare is a foregone conclusion? Not necessarily. Certain influential companies are beginning to understand that their own businesses depend on an open Internet. (Google, for example, is dependent on the ability to image the Web on its own servers, a task that might be impossible in a controlled Internet.) Activist groups like the Electronic Frontier Foundation are sounding alarms. A few legislators like Sens. Sam Brownback
of Kansas and Norm Coleman of Minnesota are beginning to look upon digital rights management schemes with skepticism. Courts might balk if the restrictions clearly violate the First Amendment. And there are pockets of technologists concocting schemes that may be able to bypass even a rigidly controlled Internet. In one paper published by, of all people, some of Microsoft’s Palladium developers, there’s discussion of a scenario where small private “dark nets” can freely move data in a hostile environment. Picture digital freedom fighters huddling in the electronic equivalent of caves, file-swapping and blogging under the radar of censors and copyright cops.

Nonetheless, staving off the Internet power shift will be a difficult task, made even harder by apathy on the part of users who won’t know what they’ve got till it’s gone. “I’ve spent hundreds of hours talking to people about this,” says Walker. “And I can’t think of a single person who is actually going to do something about it.” Unfortunately, our increasingly Internet-based society will get only the freedom it fights for.

© 2003 Newsweek, Inc.