Exhibit 28

BusinessWeek

> Close Window

SEPTEMBER 15, 2003

INFORMATION TECHNOLOGY

The Underground Internet
Members-only "darknets" are popping up to protect file-sharing from prying eyes

Around the time the Recording Industry Assn. of America said this spring it would start tracking down individuals who were trading pirated music on the Internet, Trader X, a 17-year-old U.S. high school senior who declined to provide a name to avoid prosecution, hightailed it over to a service for swapping music and other digital files called Direct Connect (DC). Trader X had used other file-sharing services in the past, but chose DC for two simple reasons: privacy and plenty of movies. In most file-sharing services, millions of computers swap files with millions of others openly online, in plain view of the RIAA and others. DC's free software lets individuals set up a password-protected, members-only network that relays music and movies among a closed group of people. "Frankly, as long as the Internet exists, file trading can't be stopped," says Trader X.

This is just one glimpse into the world of darknets -- gated communities that run on the Internet but are open only to those who belong to the private network. These mini-networks are gaining appeal among more than just teenagers looking for a free copy of rapper 50 Cent's *21 Questions*. Political dissidents from China to Iran, as well as civil liberterians in the U.S., are interested in avoiding the prying eyes of government authorities and reestablishing some privacy on the transparent Internet. Even well-respected corporations, including Hewlett-Packard Co. (**HPQ**) and Siemens, are turning to darknets to allow them to share sensitive data with outside partners while protecting the data from rivals and restricting the partners from burrowing into the corporation's own intranet.

How do darknets work? Typically, people who want to build a darknet will start by installing on their computers specialized software, which they can buy or often download for free from the Internet. Then individuals who want to form their own group swap passwords or digital keys so their computers can communicate with each other. The data shuttling between computers often are encrypted, a security feature similar to that used for online credit-card transactions. This makes darknets more secure than typical corporate intranets, since companies usually don't encrypt data. Anyone tracking the private networks could monitor the traffic, but wouldn't know what information was inside the encrypted packets. And gaining entry to a group of, say, college kids swapping music is no easy feat: Prospective members often need recommendations from friends to join.

It's a sweeping revision of the notion of the open Internet. Netizens are walling themselves off for certain activities like never before. Darknets are very different from the typical corporate networks, monoliths built to last for years. These networks are designed to be put up and taken down quickly and easily, so they can be used for a week or a year. Teenagers could establish a darknet to trade music -- and take it down as soon as they feel pressure from authorities by simply removing the software from their machines. GlaxoSmithKline (**GSK**) PLC is using a darknet so chemists, biologists, and others in-house and at some universities can share information for the development of an obesity drug.

Innovation in darknet technology is coming from many different directions. Independent developers are giving away freenet and invisibleNET, software that allows dissidents in countries where censorship exists to get information from the outside world and speak more freely among themselves. A free program called Waste, designed by America Online's Nullsoft division, showed up on the Web four months ago and is catching on among pirated-music dealers. BadBlue and Groove Networks Inc. are among the companies trying to make money from darknets. They sell collaboration software that permits a company to safely share sensitive documents or financial information with partners.

Trust among members is the critical ingredient for certain darknets, including those using technology from Waste and DC. DC is less secure than Waste because the software giving access to the main computer that runs the network is simply password-protected. If someone infiltrates a group, that person can track everything that's going on within the hub. Waste is more secure. It uses encryption to protect files and messages sent among the members of a private network, called a mesh. To join a mesh, a member exchanges encryption keys with someone in the network. Although AOL quickly yanked the software off Nullsoft's site, programmers with copies downloaded from the Web are busily enhancing it. Devotees predict the technology will blossom. "Waste will only improve over time as more users and developers adopt it," says Tom, a 22-

year-old programmer who has set up one mesh for family photos and news and another for software development.

Freenet's emphasis is on anonymity through technology, not trust. The brainchild of Irish programmer Ian Clarke, Freenet works by tying together computers around the Internet through strong encryption. Freenet organizes a bucket brigade of computers that dedicate a portion of their hard drives to encrypted data and only talk to their nearest neighbor on the network. When a request for some bit of information is made, each computer queries its neighbor to determine if it has that information. If not, the request is passed to another neighbor that the first computer doesn't know about. Freenet-China, a Mandarin translation that has been up for a year and a half, publishes news that the Chinese government would censor and allows dissidents to read banned sites, such as CNN.com. "The Internet doesn't really have all that much anonymity now," says Clarke. "People are looking for ways to share information without being watched."

Inevitably, as the pressure mounts on illegal copying, people interested in pirated-file trading are seeking out private networks. Since the RIAA started targeting individuals who are sharing files, monthly revenues of BadBlue's software designed for small-scale use, which costs between $30 and $60, have increased about 50%, says Doug Ross, the company's chief technology officer. Moreover, Clarke says that Freenet downloads have tripled during the past four months to a total of about 2 million. "As soon as [the RIAA] laid down those individual subpoenas, we started seeing posts from people looking for private networks," says Chris Hedgecock, president of Zeropaid Inc., a site where about 160,000 file sharers discuss news and exchange tips.

The entertainment industry says these digital versions of Prohibition-style speakeasies are of little concern. Since darknets typically include no more than 50 or 100 people because of technology limitations or security concerns, music and movie companies think they can't do much damage. "If they are using private networks, there is very little risk of being caught, but there is very little risk of them really doing much harm to the entertainment companies," says Randy Saaf, president of MediaDefender Inc., a copyright-protection security company.

The debate over whether limits should be put on private networks is only beginning. Just as darknets provide room for free speech or the exchange of data from pharmaceutical trials, they can also be used for black-market trading of pirated music. It's too early to tell how popular these darknets could eventually be, but the groundwork is already being laid to welcome those fleeing the public networks -- for all kinds of reasons.

By Heather Green in New York