boston.com

THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

The Boston Globe

Beating censorship on the Internet

Tools mask user IDs, give alternative routes to sites

By Hiawatha Bray, Globe Staff | February 20, 2006

While Congress battles with US Internet companies that help China restrict its citizens' Internet access, independent computer specialists are developing technologies that could reroute Internet information and put it beyond the reach of government censors.

"It was sort of a moral imperative for us to take action and do something about it," said Lance Cottrell, president and founder of Anonymizer Inc. of San Diego.

Cottrell's company is a leader in "anonymous surfing" software, which lets people go to Internet sites without revealing the location of their computers. Because it works by redirecting Internet traffic through a private computer network, anonymous surfing technology can also be used to get around blockades erected by Internet censors.

Cottrell has built a profitable business by selling this software to private citizens and businesses. But now he's working on a plan to give away anonymous surfing services to the people of China and other countries that try to censor political and religious information. "This is not a government contract," said Cottrell. "This is something we're just doing ourselves."

Meanwhile, a band of Internet volunteers headquartered in Cambridge has launched the Tor Project, which uses people's spare Internet bandwidth to help others bypass the censors. And in Canada, computer scientists at the University of Toronto are working on a similar project, called Psiphon.

Anonymizer and Tor have attracted strong support from the US government. American military and intelligence services are major customers of Anonymizer, because it lets them scan foreign Internet sites without revealing their identities. The Voice of America, a broadcasting service sponsored by the US government, uses Anonymizer to help people in Iran tune in, despite their country's efforts to block the signal.

The Tor Project is an outgrowth of research sponsored by the US Navy. "There are soldiers in the Middle East right now who use Tor to connect back to their servers in DC," said Tor project director Roger Dingledine.

Ironically, both systems make use of digital technology that the US government was fighting to suppress a decade ago. In 1993, computer scientist Philip R. Zimmermann faced a threat of prosecution for publishing Pretty Good Privacy, a data encryption program that scrambles computer files so that only the intended recipient can read them.

The government tried to prevent the release of information on encryption out of concern that criminals and terrorists would use it to conceal their activities. But by 1996, federal prosecutors dropped the investigation of Zimmermann. Now the government sees encryption and anonymous Internet surfing as powerful tools for freedom.

Anonymizer, Psiphon, and Tor all work by concealing the destination of an Internet request. Ordinarily, when someone visits a website, he reveals the numerical Internet address of the computer he is using and that of the computer he is trying to reach. This makes it easy for a censor to see what people are reading and to block access to certain Internet addresses, like those for Voice of America.

Anonymous surfing programs let users route their data through private networks of proxy machines. These machines have addresses that can't be linked to any supposedly subversive websites, so government agencies won't block them. A Chinese surfer looking for information on the banned Falun Gong spiritual movement would not go directly to a Falun Gong site, but to an innocuous-looking proxy. The request is then relayed through still more proxy machines until it reaches its final destination.

"There's no direct connection between the user in the censored country and the websites he's going to," said Nart Villeneuve, director of technical research for the Psiphon project.

The secret surfing programs also add a layer of encryption, ensuring that messages are scrambled in transit and are thus unreadable. Even if the government set up a phony Falun Gong site to trap its citizens, it wouldn't be able to identify visitors by the Internet addresses of incoming data requests. The addresses belong to the proxy computers, not the Chinese citizen.

Anonymizer has set up its own commercial network of anonymous proxies. Tor relies on volunteers to run proxy software on machines attached to the Internet.

The addresses of these machines are added to the Tor network, and data are automatically routed through them. There are about 400 Tor servers serving about 200,000 users, according to Dingledine.

But all these systems have a key weakness. Eventually, government censors will figure out the Internet addresses of the proxies and block them, thus preventing anonymous surfing.

Anonymizer addresses this by letting users subscribe to an e-mail service that sends out a daily list of the latest unblocked proxies. Cottrell admitted that government censors can get the same e-mails and move to block the proxies. But "it's a major effort," he said. "Our experience is, it takes several days."

Dingledine said that he hopes to develop software that would let users automatically find the newest open proxies. "Then we can start looking at ways to do network discovery in a way that's harder to censor," he said.

Dingledine is presently the only software engineer working full time on Tor. But Ken Berman -- manager of the Internet anticensorship office at the Broadcasting Board of Governors, parent of the Voice of America -- said that his agency may provide funding for an enhanced version of Tor, aimed at outwitting the world's Internet censors.

Hiawatha Bray can be reached at bray@globe.com. ■