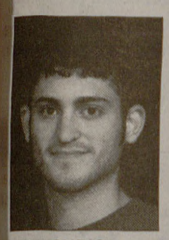
Big brother is watching

Spyware a good tool to fight terrorism



CHRIS LIVELY

The conveniences of technological evolution have definitely come at a cost to Internet users. They are now asked to take more precautions than ever when connected to the Web. Along with being subject to the growing threat of cyber crime, privacy invasion by advertisers is also a real and prevalent issue.

Spyware encompasses any program that can be downloaded on a user's computer, retrieve personal information about the user with or without their knowledge and send it to a third party. Most often used by advertisers craving marketing data, programs such as these have received rather dishonorable stereotypes as they are often responsible for the annoying pop-ups, system malfunctions and simply intruding on individuals' privacy.

But spyware tactics have also been used against the public by federal agencies as a means of security and surveillance, which has brought into light the issue regarding government intrusion of civil liberties. While Americans should never have to go out of their ways to protect their personal information for any capitalistic motif, a different scenario exists in the federal arena.

Immediately following the events of 9-11, the Patriot Act was approved by Congress, granting FBI agents greater freedom to eavesdrop on Internet activity without a court order. A more recent proposal known as the Domestic Security Enhancement Act has further sparked the issue of individual liberties versus government regulation.

One can imagine a highway free of law enforcement. However utopian this may sound for some, this situation would obviously be a chaotic and destructive one. In an effort to bring order to a situation like this, society as a whole grants law enforcement a certain amount of power in exchange for safety. The Internet highways represent an analogous scenario, but different in one important respect. Authorities on the Internet cannot be effective by simply monitoring basic day-to-day activities, as highway patrolmen do. Their techniques must be deceptive, intelligent processes that do spy on people.

Many civil rights activists protest government "snooping" activities such as those associated with spyware, claiming a violation of privacy and in turn an unconstitutional practice. While the privacy issue has been hotly debated in political arenas many times over, the issue here must be approached in a different manner. Technological criminals and terrorists often have access to the same high-tech resources as their nemeses. In a report on spyware in the Technology Review Journal, Osama bin Laden's team reportedly used the tactic of hiding one type of data file within another. Essentially, a text file with attack plans can be hidden in a photo of Britney Spears. Situations like these make the need for advanced counter-terrorism technology more than apparent.

The government increased online surveillance as it implemented technologies such as Carnivore and Echelon. Carnivore was responsible for tracking down terrorist activities and detaining 400-500 suspects immediately following the attacks on the World Trade Center in 2001. Despite the programs' occasional flaws in mistaking implicating an innocent person, it is still better to exhaust all possibilities than to miss one.

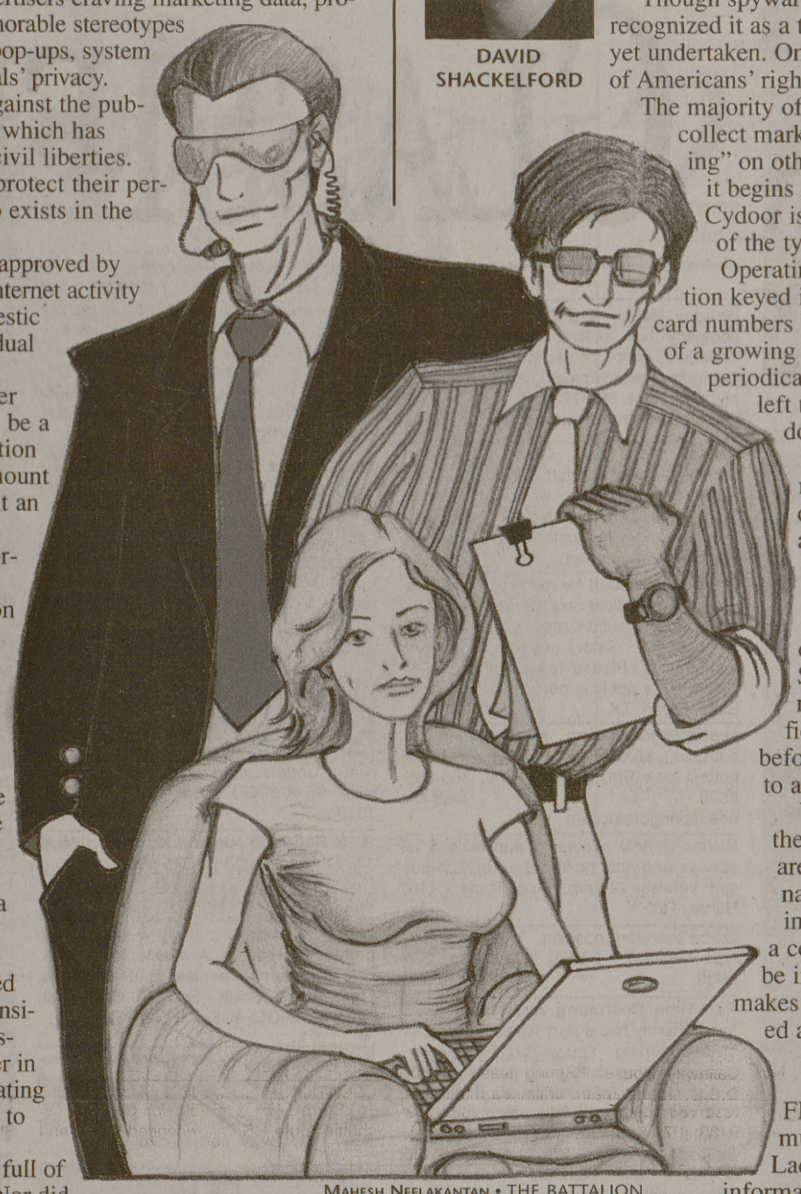
The writers of the Constitution probably did not foresee a land full of machines that can send messages from coast to coast in seconds. Nor did the idea of foreign terrorists wreaking havoc on the soon-to-be-built cities and civilizations ever cross Ben Franklin's mind. Post-9-11 America is a whole new scenario.

It is true that not every seemingly logical response to terrorism is a reasonable solution that should be enacted. However, at a time when national security should operate to its fullest capacity, people will have to sacrifice for a greater cause. This is not to say people should assume and invest all authority and credibility in federal agencies, for they have been deceptive and shady at times. But the uncertainty of a federal agency in collecting online user information is a far better circumstance than that of the certain intentions of a terrorist being unleashed.

Spyware and other surveillance tactics are a vital contribution to America's security and well-being. These security services do come at a cost, however. But this cost is a relatively small one when one contemplates the potential security benefits that spyware and its counterparts offer people.

America has a long way to go in combating foreign and domestic terrorists. But only with a more centralized intelligence community working in sync with better technology can real homeland security be established. Spyware can perhaps be seen as a prototype of the new security measures that are necessary today.

Chris Lively is a senior sociology major.



MAHESH NEELAKANTAN • THE BATTALION

Use of spyware violates right to privacy

DAVID SHACKELFORD

Internet users are having to learn more ways to secure their systems as more ways to breach them are being created. Spyware is one of the latest of these creations and has recently earned itself a place among the most irritating of security breaches. Spyware refers to any programs used to monitor activity and gather user information. As the name implies, these programs perform their functions without users' knowledge.

Though spyware is better known for its commercial use, the government has recognized it as a tool to facilitate one of the greatest eavesdropping campaigns yet undertaken. Once again the war against terror is being waged at the expense of Americans' right to privacy.

The majority of spyware's publicity refers to its use by corporate advertisers to collect marketing data. It gets onto a PC most commonly by "piggybacking" on other programs users download from the Internet. Once installed, it begins gathering information from Web activity to key strokes. Cydoor is a prime example. This program is tagged onto KaZaa and is of the type of spyware companies prefer to call "adware."

Operating undetected, spyware has the ability to capture any information keyed into an online form, including Social Security numbers, credit card numbers and passwords. Spyware can be dealt with by employing one of a growing number of detection and removal utilities. This has to be done periodically as long as downloading continues. As long as spyware is left to accumulate, it takes up space on the hard drive and slows down a computer.

Though companies whose programs include spyware are required to notify users, the nature of their purpose calls for deception. According to cexx.org, spyware enters computers and collects information in a deceiving manner. Also, companies use slick spyware and legal teams that can bury spyware's usage in a license agreement.

Growing concern about these deceptive tactics has prompted work on the Spyware Control and Privacy Protection Act. Sen. John Edwards, D-N.C., intends for the bill to require clear notice of spyware in license agreements. Users would be notified of the presence and precise use of a spyware program before they download. However, this refreshing bill is only tailored to address companies.

While many are looking forward to when the current use of these programs is classified as a federal offense, the FBI and CIA are using their own forms of spyware to snoop in the name of national security. The FBI-developed Carnivore tracks e-mail, instant messages and Web search trails and relays information to a centralized database. The FBI maintains that Carnivore can only be installed after obtaining an appropriate court order. The court makes certain that only specified target information will be intercepted and copied.

This doesn't always happen, however.

According to a Federal Computer Week article, an internal FBI memo sent in April 2000 said "Carnivore intercepted so much unrelated e-mail during its investigation of Osama Bin Laden that the FBI stopped using it and may have destroyed information it collected related to the terrorists."

No one should expect an investigation of such massive proportions conducted on such untamed terrain to be painless. Many Americans agree that some sacrifice of privacy is necessary to pursue terrorists hiding among the general population. But until government spyware proves dependable, Americans must ask themselves if the compromise is worth it.

The FBI and CIA, under the guise of the Total Information Awareness Office, have overwhelming power to conduct mass surveillance. All record of personal information and Internet activity is within their grasp. Perhaps not ironically, this capability is being exercised under an administration that has one of the worst reputations for withholding government information.

If Americans stand down and allow this one-way trend to continue, the implications for future invasions of privacy are enormous.

Fighting terrorism is a formidable task and worthy of utmost priority. National security is at the forefront of American consciousness. A sense of security must, however, be weighed against those fundamental principles that ensure civil liberties. If those principles are neglected, even if government spyware does succeed, the United States may end up a secure nation with an insecure people.

David Shackelford is a senior journalism major.

MAIL CALL

Demonstration a venue to exchange ideas

In response to Nov. 20 mail call:

Expressing "disgust" for Young Conservatives of Texas' anti-diversity protest is a clear indication that Mr. Foster completely misunderstood its intention. The protest was not an attack on any one individual or group, but rather a venue for the exchange of ideas. Implying that we make Aggies look *ignorant and hateful* couldn't be further from the truth.

In fact, if one had taken the time to attend the protest and listen to some of the discussions, they would know that it was productive as well as educational. I personally had some great conversations with a few of the guys from Beta Xi Chi (a multicultural fraternity). I found that we share more common ground than I anticipated and that they helped me to better understand their points of view.

Mr. Foster's feelings of embarrassment, or that our campus is unfriendly to anyone, are his own and are not the consensus at Texas A&M.

Aaron Dunn
Class of 2003

University officials hurting Aggie Spirit

In response to a Nov. 20 mail call:

Mr. Kibler wrote, "Texas A&M did not create Aggie Spirit of Aggie traditions. They exist or do not exist because of the students." How can you say that traditions such as Aggie Bonfire do not exist because of the students? These traditions take place on the A&M campus, therefore the University should take responsibility for the activities that occur. If dangerous things were happening during these activities, such as consumption of alcohol, that is the University's fault for not providing rules and regulations for these events and not enforcing existing ones. It is the former president's fault for taking away these traditions, not the students.

How are we as students supposed to keep the Aggie Spirit alive when figure heads such as yourself keep taking traditions along with their spirit away? To conclude, we should not have to ask ourselves as students what we are going to do to keep the spirit alive. You and other leaders of this University should ask yourselves what can you do or stop doing to keep the spirit alive. The responsibility rests on your shoulders.

Jourdan Newman
Class of 2006

Justice system must be ruled by moral men

In response to a Nov. 21 mail call:

There has been quite a hysteria over the recent removal of Judge Moore from the Alabama Supreme Court. It is obvious that Judge Moore was in defiance of the established order, and according to principles of law, should be removed from his position for his actions. But take a look at the bigger picture. Moral debasement from the law nullifies the law's function.

Founding fathers Jefferson and Franklin (unacclaimed "Christian" men, more to the tune of atheist and agnostic) stated that the Constitution and its justice system would only endure if it remained in the hands of moral men. To advocate justice without morality is to produce a failure within the system.

Rome, France and other empires systematically removed morality from their justice system until nothing was left but law, and broken empires. Can we "legally" throw men like former Judge Moore from the courts for advocating morality in law? Sure we can, but we're encroaching into an experiment of dissenting justice without ethics — and 30, 40 or 50 years from now we may find ourselves in an extremely difficult position from which to rule.

Joseph Couch
Class of 2003

Withdrawing petition the right thing to do

In response to a Nov. 21 article:

My attempted recall of Sen. Dustin Teems did not "fail" in the sense that the student body found it to be baseless, but rather I chose to withdraw it because it was the right thing to do. At the time I initiated the recall, it was because I felt that Sen. Teems was not acting in the best interests of his constituents due to his comments in opposition to the Open Access to Budget bill. However, Sen. Teems and others were under the impression that a University rule restricting access to the SGA budget existed. I would not have attempted a recall had the SGA leadership acted with due diligence and not told the student body that such a rule existed, when in fact there was no such rule.

When it became obvious to me that Sen. Teems was not acting in a negligent manner, but was a victim of the SGA's operational deficiencies, I withdrew the petition. Showing his dedication to serving the student body, he has even gone on to work with me, and several others, on a bill that would prohibit the student senate from voting by secret ballot, as they have done on several recent occasions.

Mark McCaig
President SGA Watch

The Battalion encourages letters to the editor. **Letters must be 200 words or less and include the author's name, class and phone number.** The opinion editor reserves the right to edit letters for length, style and accuracy. Letters may be submitted in person at 014 Reed McDonald with a valid student ID. Letters also may be mailed to: 014 Reed McDonald, MS 1111, Texas A&M University, College Station, TX 77843-1111. Fax: (979) 845-2647 Email: **mailcall@thebattalion.net**