

# Internet surveillance system protects nation



John Deans

Our family had two great Thanksgiving meals in a single day this year and we all had a wonderful time. It was marred though by the tragic news of the Mumbai, India slaughter by 10 Islamic butchers who murdered around 172 people and injured another just as many.

That is almost a 17-to-1 kill ratio and since it lasted for almost four days these guys were dead-enders whose only goal was to kill as many innocent people as possible. India had no early warning or intelligence that this attack was coming which ended up catching them in complete surprise.

With all my complaints about President Bush, at least he has successfully protected our country from another deadly sudden attack over the past seven years. Many attempts have been thwarted such as the Fort Dix Six who schemed and prepared to wipe out hundreds at one of our Army Bases in New Jersey.

Luckily there was a brave IT guy at Best Buy who dupes DVDs who tipped the FBI about the terrorists' plan after the idiots filmed themselves on a camcorder training for the attack.

The good thing about living here in Texas is that a terrorist

gunmen attack would be both unlikely and probably unsuccessful since there would be numerous true Texans with their legally concealed handguns to accurately return fire. That said, the last thing we want to have to do is battle these barbarians in our hotels, malls, or God forbid, our schools.

Intelligence is absolutely critical to proactively stopping these horrible assaults before they are carried out. This vital intelligence is largely gathered from digital pipes that carry voice and data. That group of pipes is the Internet.

Since 2001 our government has stopped numerous attacks on our country by intercepting communications over the Web. This high tech snooping of e-mails, chat sessions, VoIP calls (Voice over Internet Protocol)

and message boards has been controversial but quite effective.

One of the early Internet surveillance systems implemented by the FBI was called Carnivore which was implemented during the Clinton administration.

The Carnivore system is basically a PC running specialized software that "packet sniffs" all Internet traffic coming and going through an Internet service provider (ISP). Most every ISP had to have this snooping system installed and available to the FBI at all times.

Before you get your civil rights and privacy feathers ruffled, the FBI is not continuously listening and logging everyone's e-mails and Web surfing. The FBI has to have a reasonable suspicion that someone is engaged in criminal activities and request a court order to view the suspect's online activity.

Only then a court grants the request for a full content-wiretap of e-mail traffic only and issues an order.

It is at that point the FBI contacts the specific ISP that is supplying Internet service to that suspect to provide filtered traffic data gathered from the Carnivore system. That data is

filtered based on the IP (Internet protocol) address for the location of the suspect. Then the data is placed on a portable hard drive and picked up by the FBI for analysis.

The warrant is for a limited amount of time, targeted to a specific person at a particular IP address, for only certain types of Internet activity.

Back in 2005 the original Carnivore system was replaced with a more off-the-shelf system that performs the same function as the older packet capturing software packages based on Packeteer and Coolminer.

All of our local ISPs such as AT&T DSL, SuddenLink Cable and even Texas Broadband wireless have these new Carnivore Internet surveillance systems installed and ready to use. Do not fuss at them for this since they had to comply under penalty of law.

These wire tapping laws are based on Communications Assistance for Law Enforcement Act (CALEA) which was introduced in 1994 and more recently in 2008 the Foreign Intelligence Surveillance Act, known as FISA.

There is a technological cat and mouse game between the feds and the terrorists with both continuously modifying, upgrading and morphing their

software and hardware.

We have the bad guys wanting to communicate and coordinate their evil deeds, the feds electronically chasing them to prevent those dire operations from being carried out, and then we have the ACLU and the *New York Times* screaming privacy invasion. Ever wonder whose side those two are on?

The big digital nut to crack now is the VoIP channel. With very low cost, if not free, Voice over Internet services like Vonage and Skype, the feds have their hands full sifting through all those billions of Web conversations to find that one chatter thread about an impending terrorist attack on our shores.

There is a long-rumored yet unconfirmed account of an Internet sniffing operation under way being conducted by the NSA (Nations Security Administration) which has a highly advanced array of supercomputers and top secret decryption software that would be capable of tapping Internet voice communications.

Vonage is easy since their voice traffic is not even encrypted, but the more popular Skype network is strongly encrypted which would require an NSA level operation to successfully tap into it.

Since I do not send or receive

e-mails or have Internet conversations with Islamic radicals, I do not worry if my digital conversations are being monitored by the government. They have their hands way too full to monitor a high tech harmless yahoo like me.

Bottom line: The primary responsibility of our national government is to protect its citizens. Authorized Internet snooping is a vital tool that our federal authorities must have and use reasonably to be able to prevent a Mumbai India attack from happening here in the USA.

Next week's column: 2008 Christmas list.

*John Deans of DeansConsulting.com is a Brenham area computer networking consultant who can be reached at 289-2233 or John@DeansConsulting.com for questions and comments.*