

Battle Over Your Inbox: Why the FBI Wants Snooping Rights

Magician Penn Jillette once said his favorite thing about the Internet was that he gets to go into the private world of real creeps without having to smell them. The danger with the FBI's new email snooping program is that they could sniff through your email whether you're a real creep or not. The future of electronic communication now rides on striking a workable balance between giving crime-fighting tools to the government and privacy guarantees to netizens.

Email lost its novelty status long ago. The primary reason why people use the Internet today is for sending and receiving email. With the passage of the digital signatures laws, email will become an even more critical, and sensitive, part of daily communication. The program is designed to intercept communication to and from people who are part of a criminal investigation. The FBI and the NSA have a history of trying to introduce products and services that compromise the security of an individual. The by now infamous *Clipper* Chip is a prime example. This chip, also known as MYK-78T, is an NSA designed, tamper-proof VLSI chip designed for encrypting voice conversations. Each chip has a key used to encrypt a copy of each user's message key. As part of the synchronizing process, the sender Clipper chip sends a copy of the current session key, allowing a government eavesdropper to recover the session key. Using this, the message can be recovered. The government encouraged the sale of these telephones. This could enable them to collect huge databases.

Now let's look at how Carnivore works and why you should be worried.

THE TECHNOLOGY

Carnivore started as an off-the-shelf email program. It was later modified by the FBI. The FBI will never say what program their sniffer is based on, but sources say that the program was AG Group's EtherPeek. The FBI's sniffer is also known as a packet filter. It looks for packets of data, such as an email, that travel along a network. It can also monitor visits to Web sites. Once installed at an ISP, the setup allows the FBI to remotely check up on or change who they are monitoring. The FBI merely intercepts the message, copies it and sends it along its way. Hence there is no danger to the packet of data being lost or garbled. The FBI has a copy of *everything* that passes through the gateway.

THE DANGER

The questions about Carnivore are coming fast and furious from privacy advocates.

- Can it point to innocent users?
- How often is it used?
- Under what circumstances can it be used?
- Is it hooked permanently to service providers?
- Who keeps a record of who is being monitored?

But that's not all.

The FBI says the program only captures communications going to or from its target, including successfully distinguishing between emails from different family members. But since the FBI has not released the source code for the program, we are all left to take the FBI at its word that Carnivore catches only the communications of its intended target.

WHAT'S NEXT

It's unlikely the FBI will release its source code for the program. But there are more reasons you should be worried about government -- or your employer -- peeking at your email.

- Many governments around the world want changes in law that let authorities eavesdrop on the Internet more easily. It would make tapping into email subject to the same oversight as wiretapping somebody's phone. They argue that this provides for better privacy protection.
- Legislations will also be passed which would make it binding on the companies to tell their workers if they are being monitored.

Electronic communication is already the way individuals and businesses chat, exchange information and conduct million-dollar deals. The FBI should be able to catch bad guys, but there is something fishy in the move to monitor the inboxes.

Is Carnivore a threat to freedom or a useful law enforcement tool?