

Search  
[Advanced Search](#)

- [Home](#)
- [Pay & Benefits](#)
- [Management](#)
- [Homeland Security](#)
- [Defense](#)
- [E-Government](#)
- [Per Diems & Travel](#)
- [Jobs & Careers](#)
- [Procurement](#)
- [A-76 & Outsourcing](#)
- [Life After Government](#)
- [GovExecTV](#)
- [Bill Tracker](#)
- [Calendar](#)
- [Fedblog](#)
- [Mailbag](#)
- [Print Subscriptions](#)
- [E-Newsletters](#)
- [Events & Awards](#)
- [Editorial Calendar](#)
- [Media Kit](#)
- [Reprints](#)
- [FAQ](#)
- [Privacy Policy](#)
- [About Us](#)
- [Contact Us](#)

**DAILY BRIEFING**

April 10, 2006

**Internet devices threaten NSA's ability to gather intelligence legally**

By Shane Harris, [National Journal](#)

Among the threats facing the National Security Agency are Al Qaeda, the Iraqi insurgency, and eBay.

Yes, eBay, the online auction house. Not because its members sell state secrets, but because of a company that eBay purchased last year -- Skype.

Skype is an online service that lets people converse through their computers. Its 75 million users place voice calls over the Internet. The calls sound clear. They're free, because phone carriers aren't used. And because of the Internet's diffused architecture and its facility for privacy, Skypesters' identities, their locations, and the substance of their conversations can be undetectable. This is not what the NSA's worldwide eavesdroppers want to hear.

Skype and other widely used Internet communications devices, including e-mail, threaten the NSA's ability to gather intelligence and to do so legally. For more than four years, without warrants and by order of President Bush, the agency has hunted for terrorists by intercepting communications between people in the United States and people abroad possibly connected to terrorism.

The legality of that order is being hotly debated in Congress. Bush says that the 27-year-old Foreign Intelligence Surveillance Act, which governs domestic eavesdropping for intelligence purposes, doesn't adequately address Internet-based communications.

In the opinion of some legal scholars and intelligence practitioners, lawmakers haven't faced this fact. Until they do, the NSA remains on shaky legal ground and at a strategic disadvantage against terrorists, who may rely on the Internet above all other tools for plotting their attacks.

When FISA became law in 1978, even rudimentary e-mail was years away from use. The law "did not anticipate the development of global communications networks," according to Kim Taipale, a technology law scholar and a member of the Task Force on National Security in the Information Age, a nonpartisan panel supported by the Markle Foundation that has produced widely praised assessments of technology's role in counter-terrorism.

"Thirty years ago ... it made sense to speak exclusively about the interception of a targeted communication -- one in which there were usually two known ends and a [phone line] that could be 'tapped,' " Taipale writes in an upcoming essay for the *New York University Review of Law and Security*.



- **Printer Friendly Version**
- **E-mail this Story to A Friend**
- **See Readers' Comments/ Add Your Own**

**RELATED STORIES**

- [Justice Department responds to lawmakers' wiretapping probe](#) (03/27/06)
- [NSA program broader than previously described](#) (03/17/06)
- [Senator may address spying concerns in supplemental funding bill](#) (03/07/06)
- [Gonzales fulfills expectations of supporters, doubters](#) (03/03/06)
- [Controversial counter-terror program lives on](#) (02/23/06)

Phone calls travel over a dedicated circuit, in easily traced paths.

But Internet communications are broken down into discrete units, called packets, that swirl through the global network along different, sometimes circuitous routes before being reassembled at their destination. If placing a phone call can be likened to mailing someone a letter, sending an e-mail is like cutting that letter into 50 pieces and dividing them among several couriers, and then asking the couriers to reassemble the letter upon delivery.

To intercept packets, devices called "sniffers" are placed at various communication nodes to scan traffic as it passes, looking for interesting packets and, hopefully, reassembling them coherently. If the NSA has an e-mail address to target, catching the message is relatively simple -- put a sniffer near the user's Internet service provider.

But the NSA's warrantless eavesdropping program also involves looking for suspicious patterns in a sea of communications. The NSA might not know what it's looking for, so it has to examine a lot of data. Put another way, "If you can't find the needle, you have to take the haystack," said Doug Graham, a security expert with BusinessEdge Solutions and a former surveillance-systems operator with the Royal Air Force.

The NSA's program is fundamentally unsuited for FISA, administration officials contend. The law requires the government to develop a reasonable basis to believe that a specific individual or a source is an agent of a foreign power, and then apply to a special court for authorization to pursue that target. It's a "cumbersome mechanism" that doesn't provide for technical methods such as automated packet sniffing, which could uncover suspicious activity in the first place, Taipale writes.

Legislative efforts to address the NSA program have come from Sen. Mike DeWine, R-Ohio, and Senate Judiciary Committee Chairman Arlen Specter, R-Pa., who rejects the Bush administration's argument that the FISA court has no jurisdiction over what the White House calls the "terrorist surveillance program."

Specter wants the court to review the program, and DeWine would place limits on NSA's warrantless work. But neither senator proposes making significant amendments to FISA itself, and they provide no new approach that would make new kinds of eavesdropping legal and yet still allow for monitoring by the courts.

"FISA is triggered by foreign intelligence collection conducted 'within the United States' or against 'U.S. persons,'" Taipale writes. But by design, the Internet recognizes no boundaries, and it treats anonymity and deregulation as attributes. Ordinarily, the NSA must answer two questions before it can eavesdrop: Where is the target, and what is his nationality?

"The borderless nature of terrorist threats and global communications has made place-of-collection and U.S. personhood an increasingly unworkable basis" for gathering intelligence, Taipale argues. Still, the Bush administration insists that warrantless surveillance occurs only when at least one party to a communication is outside the United States.

But how can the NSA be sure? Graham explained that a terrorist sending an e-mail from Iraq could mask his location by sending the message through a sort of gateway, known as a user agent, which hands off the message to an Internet service provider. If the user agent is based in, say, California, then the service provider thinks the message came from California, not Iraq, Graham said.

It's unclear to what extent Internet service providers are cooperating with the NSA. But in Graham's example, it's possible to see how the agency might think that a message that originated overseas was purely domestic, and hence ignore it. Officials have said that the NSA doesn't intercept communications without warrants when both parties are inside the United States. So, theoretically, a terrorist in Iraq could communicate undetected with a terrorist in California.

In his essay, Taipale writes that FISA "contemplates only a single threshold for authorizing interception" -- reason to believe that someone is an agent of a foreign power.

According to officials familiar with the NSA program, the agency broadly monitors information such as an e-mail's route -- at least as much as can be traced -- and the time of day it was sent to establish patterns of suspicious activity. These patterns can be detected through automated programs and without humans seeing the data. With "some approved procedure that identifies potential threats and allows for some limited follow-up," the NSA program could be regulated, Taipale maintains.

Precedent exists for such limited but legal searches and surveillance. Under a "Terry stop," police officers can briefly detain someone for questioning and conduct a limited pat-down search if they have "reasonable suspicion" to believe the person may be involved in a crime. It is one step short of an arrest, yet it gives police some ability to seek more evidence. (The name stems from the 1968 Supreme Court case, *Terry v. Ohio*, that affirmed its legality.)

"What is needed ... is the electronic surveillance equivalent of a Terry stop ... an authorized period for follow-up monitoring or investigation of initial suspicion derived from automated monitoring," Taipale says. "If the suspicion is not justified on follow-up, monitoring is discontinued. However, if suspicion is reasonable, then monitoring continues."

Taipale's essay, to be published in June, has attracted some early response. One FBI official called the analysis of FISA's deficiencies "brilliant," and a former government official experienced in intelligence-gathering called Taipale's recommendations "right on the mark."

Taipale didn't suggest any new legal standards for conducting limited surveillance. But in the *Terry* case, then-Chief Justice Earl Warren set down the rules of the process: "In justifying the particular intrusion, the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."

But can lawmakers learn enough about the NSA's domestic eavesdropping activities to make a well-informed decision on how to better control them? NSA's critics say it's premature to change FISA when members don't understand the program and the Bush administration won't reveal its operational details.

Taipale's suggestion, while "insightful," is "based on pure conjecture," said Bruce Fein, an associate deputy attorney general in the Reagan administration. In theory, electronic surveillance might benefit from Terry stops, Fein said, but "what's worrisome ... is, we don't have a ghost of an idea what are the criteria to trigger the NSA to target you or me."

---

[Back to Top](#) | [Home](#) | [Top E-Mailed Stories](#)

©2006 by National Journal Group Inc. All rights reserved.