NSA shifts to e-mail, Web, data-mining dragnet

Recent reports say the National Security Agency is more focused on surveillance of e-mail, Web browsing, and search terms than ever before.

by **Declan McCullagh** March 11, 2008 4:00 AM PDT

The National Security Agency was once known for its skill in eavesdropping on the world's telephone calls through radio dishes in out-of-the-way places like England's Menwith Hill, Australia's Pine Gap, and Washington state's Yakima Training Center.

Today those massive installations, which listened in on phone conversations beamed over microwave links, are becoming something akin to relics of the Cold War. As more communications traffic travels through fiber links, and as e-mail and text messaging supplant phone calls, the spy agency that once intercepted telegrams is adapting yet again.

Recent evidence suggests that the NSA has been focusing on widespread monitoring of e-mail messages and text messages, recording of Web browsing, and other forms of electronic data-mining, all done without court supervision. Taken together, those activities raise unique privacy and oversight concerns greater than those posed by large-scale monitoring of voice communications.

Documents released last week by a security consultant (**PDF**

) indicate that an unnamed major wireless provider has opened its network to the U.S. government, allowing customers' e-mail, text messaging, and Web use to be monitored. And Assistant Attorney General for National Security Kenneth Wainstein **said**

last week that surveillance of e-mail was the real concern raised by the debate over amending the Foreign Intelligence Surveillance Act.

That led some high-ranking House Democrats, including Energy and Commerce Chairman John Dingell, to circulate a letter (**PDF**

) advising their colleagues to look skeptically at a Republican proposal that would grant retroactive immunity to companies that illegally let the Feds plug into their networks. The Republicans' blanket of retroactive immunity **would likely cover**

e-mail providers, search engines, Internet service providers, and instant-messaging services too.

On Monday, the *Wall Street Journal* published **an article**

providers, and instant-messaging services too.

On Monday, the *Wall Street Journal* published **an article** saying that the NSA can, "without a judicial warrant," obtain the Subject line and other header information from e-mail messages, plus information about Web sites visited and queries to search engines. Phone records, credit card usage information, and airline passenger data are also reportedly vacuumed up by the NSA.

"According to current and former intelligence officials, the spy agency now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records. The NSA receives this so-called 'transactional' data from other agencies or private companies, and its sophisticated software programs analyze the various transactions for suspicious patterns," the article said.

For its part, the NSA says that it abides by U.S. law. Last week, Donald Kerr, the principal deputy director of national intelligence, blamed critical reports on the NSA's culture of "stand-offishness" and said "we've lost something we never knew we needed until we didn't have it--the support of a grateful nation. The question we have to ask now, and this is something everyone here should help think about, is how do we get it back?"

If the reports are correct, what this transactional-data-dragnet amounts to is a rebuilding of the Defense Department's Total Information Awareness program, which promised to do extensive warrantless data-mining to identify "information signatures" that could identify criminals. After a public outcry, the department renamed it Terrorism Information Awareness; Congress **zeroed funding** for it in September 2003.

But that law referred only to "the program known either as Terrorism Information Awareness or Total Information Awareness, or any successor program"--leaving the door open, given sufficiently clever lawyering, to a *similar* program that wasn't quite close enough to be called a "successor" to TIA.

Elements of this data dragnet have been disclosed before. *USA Today* **reported** two years ago on how the NSA has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon, and BellSouth; the latter two have narrowly **denied it**. Qwest reportedly was **approached** but rejected the request.

A **survey** CNET News.com published in February 2006 asked the major telecommunications and Internet companies this question: "Have you turned over information or opened up your networks to the NSA without being compelled by law?" AT&T, Adelphia, Google, Level 3, Verizon, and Yahoo would not answer the question; the rest said they had not.

A subsequent **article**

not answer the question; the rest said they had not.

A subsequent **article** by Seymour Hersh in the *New Yorker* said the NSA had returned to "intercepting large numbers of electronic communications made by Americans"--the same kind of legally dubious tactic that led to the Foreign Intelligence Surveillance Act being enacted in 1978.

FISA reinforced the notion that the NSA could conduct widespread surveillance of foreigners, but specified that a court order (or authorization from the attorney general) was needed to spy on American citizens. That means the world's largest intelligence agency is, legally speaking, on very shaky ground when operating its e-mail/text-messaging/Web-site-visiting/search-term dragnet.

The Electronic Frontier Foundation's Kurt Opsahl posted a **stinging critique** of the data-dragnet's legality. Here are some excerpts from what Opsahl wrote, referring to the *Journal* article:

The infobox incorrectly asserts that the subject lines of email are not "content," and can be obtained without a warrant... But this is contradicted by the Department of Justice's own 2002 Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations manual, which states that "the subject headers of e-mails are also contents."

The infobox incorrectly asserts that the NSA can review "[s]ites visited and searches conducted" without a warrant. "According to current and former intelligence officials, the spy agency now monitors huge volumes of records of ... Internet searches." "The [NSA's] haul can include ... records of Internet browsing." To the contrary, courts have held that search terms are "content" within the meaning of the Electronic Communications Privacy Act.

The infobox asserts that the NSA can ***get cellphone location data*** *without a warrant. "The information [obtained by the NSA] can give such transactional information as a cellphone's location..." The issue of obtaining cell phone location information has been contentious for some time, but the vast weight of judicial interpretation is that a probable cause warrant is required.*

If you get the feeling that a lot of this depends on a set of legal definitions that the NSA would like to keep as fuzzy and ambiguous as possible, you're probably right.

One thing the recent disclosures are likely to do is put the Bush administration on the defensive, which will happen just as Congress is **preparing** to vote on extending retroactive immunity to telecommunications companies. It has looked likely to pass if the House Democratic leadership had held an up-or-down vote; the Senate **already approved its version** by a 68-29 margin.

leadership had held an up-or-down vote; the Senate **already approved its version** by a 68-29 margin.

Add in FBI Director Robert Mueller's **acknowledgment** last week of additional surveillance abuses, and his **admission** that retroactive immunity may not be all that necessary, and retroactive immunity looks a lot less compelling a prospect than it did a week ago. Then again, the NSA didn't need it to create an electronic dragnet in the first place.

Cullagh

h is the chief political CNET. Declan previously was a reporter for Time and the Washington bureau chief for Wired and wrote the Taking Liberties section and Other People's Money column for CBS News' Web site.