Behind the legal fight over NSA's "Stellar Wind" surveillance

New disclosures about the NSA's extrajudicial surveillance program—and the lawyer who blew the whistle on it—shed light on a legal fight within the government.

By Julian Sanchez | Last updated December 16, 2008 10:25 PM

The most recent edition of *Newsweek* confirms a few long-held suspicions about the National Security Agency's controversial post-9/11 surveillance activities—such as the identity of the Justice Department lawyer who first tipped off *The New York Times* about the administration's warrantless wiretapping and the basis for the internal showdown that led to a now-infamous face-off at the attorney general's hospital bed. It also provides a few new revelations—including the classified name of the program: "Stellar Wind."

In a lengthy profile in the magazine's December 22 issue, Michael Isikoff names Thomas M. Tamm, formerly an attorney with the Justice Department's Office of Intelligence Policy and Review, as the ur-source of the earthshattering *New York Times* story that first revealed the existence of a secret program of warrantless surveillance authorized by the president in the aftermath of the 9/11 terrorist attacks.

This is not the first time Tamm has been named as a potential source of reporting on the NSA program. Indeed, Isikoff himself first did so over a year ago, in a *Newsweek* story describing an FBI raid on Tamm's home. It is, however, the first time that Tamm himself has spoken publicly about his role in the leaks, or discussed his reasons for coming forward.

Perhaps surprisingly, the man whose phone call ultimately led to the program's exposure knew very little about it at the time. Against the swelling blogospheric chorus calling for his head—or the quieter but more ominous federal prosecutors who may yet join the choir—Tamm can argue that he never disclosed any operational details of "the program," which only a few ultra-insiders were familiar enough to call Stellar Wind. After all, he didn't *know* any operational details. Whatever specifics the *Times* got presumably came from one of the other dozen or so anonymous sources who spoke to the paper.

All Tamm knew was that something "didn't smell right" about an odd second track for wiretap requests that passed through his office—requests that could only be signed by the Attorney General. When he started raising questions, a superior told him not to poke around—and that the "AG-only" program was probably illegal.

"I thought this [secret program] was something the other branches of the government—and the public—ought to know about," Tamm told *Newsweek*, "So they could decide: do they want this massive spying program to be taking place?" Now, however, the magazine is able to describe Stellar Wind in at least rough outlines:

> The NSA identified domestic targets based on leads that were often derived from the seizure of Qaeda computers and cell phones overseas. If, for example, a Qaeda cell phone seized in Pakistan had dialed a phone number in the United States, the NSA would target the U.S. phone number—which would then lead agents to look at other numbers in the United States and abroad called by the targeted phone. Other parts of the program were far more sweeping. The NSA, with the secret cooperation of U.S. telecommunications companies, had begun collecting vast amounts of information about the phone and e-mail records of American citizens. Separately, the NSA was also able to access, for the first time, massive volumes of personal financial records—such as credit-card transactions, wire transfers and bank withdrawals—that were being reported to the Treasury Department by financial institutions. These included millions of "suspicious-activity reports," or SARS, according to two former Treasury officials who declined to be identified talking about sensitive programs. (It was one such report that tipped FBI agents to former New York governor Eliot Spitzer's use of prostitutes.) These records were fed into NSA supercomputers for the purpose of "data mining"—looking for links or patterns that might (or might not) suggest terrorist activity.

In a related article in the same issue, *Newsweek* confirms that, as *The New York Times* first reported last summer, it was this data mining program that provoked a near-mutiny within the Justice Department, culminating in a dramatic showdown at the hospital bedside of an ailing Attorney General John Ashcroft between then–White House Counsel Alberto Gonzales and acting AG James Comey.

The data-mining component of Stellar Wind was first revealed by *USA Today* in 2006, nearly five months after the initial *Times* story about warrantless wiretapping broke. The wiretapping described by the *Times* came to be known as the "Terrorist Surveillance Program"—a term that seems to have been invented after the fact to allow officials to testify before Congress on the aspects of Stellar Wind that had been exposed without admitting to any of the activities that hadn't yet come to light.

While the TSP purportedly involved recording the actual contents of American targets' international communications, the data mining program cast a far broader net, sweeping in by the millions "the telephone numbers of callers and recipients in the United States, and the time and duration of the calls" as well as "the subject lines of e-mails, the times they were sent, and the addresses of both senders and recipients." This "metadata" dragnet purportedly sucked up the information equivalent of an Encyclopedia Britannica every four seconds.

With that much confirmed, we can speculate a bit as to what might have sparked the rebellion at Justice. Though it is NSA wiretaps that have received the most attention, it seems that DOJ attorneys must have largely accepted the theory that the president's inherent powers under Article II of the Constitution allowed him to ignore the requirements of the Foreign Intelligence Surveillance Act when it came to intercepting international communications. But the data mining program appears to have had a much broader scope. It was the legal justification for this data collection, cooked up by überconservative attorney John Yoo, that appears to have raised the eyebrows of his successor at the Office of Legal Counsel, Jack Goldsmith.

Newsweek declines to get into what it calls the "mind-numbing" specifics, but says that the nub of the rebellion at Justice stemmed from Goldsmith's conclusion that the data mining program constituted "electronic surveillance" under the terms of FISA. That suggests that Yoo's analysis—of which Comey would later say "no lawyer reading that could reasonably rely on it"—had sought to somehow deny that such sweeping collection constituted electronic surveillance. Yoo may have been reluctant to rely exclusively on the Article II trump when dealing with vast quantities of domestic communications between parties not even suspected of terror ties.

The question is how anyone could possibly make that claim with a straight face. Fourth Amendment jurisprudence has traditionally distinguished between protected "content" and constitutionally unprotected "non-content" information about communications. The latter category would include most of the "metadata" swept up by the data mining program, but the Justice Department's own computer search manual defines e-mail subject lines as "content," as they routinely convey something about the "meaning or purport" of the communication.

In a way, though, that's beside the point, because as George Washington University law professor Orin Kerr observes, FISA defines "content" far more broadly than the Fourth Amendment does. Not only is "metadata" clearly included in the FISA definition of "content" whose interception constitute "electronic surveillance," but the statute spells out specific "pen register" and "trap and trace" procedures by which intelligence agencies are to seek judicial approval to acquire such information, subject to less stringent standards than must be met for full-blown wiretaps.

Even if some clever way were found to circumvent the requirements of FISA, there's the Stored Communications Act, which explicitly makes it a crime to "knowingly divulge a record or other information pertaining to a subscriber to or customer of such service... to any governmental entity."

So how could Yoo—or anyone—conceivably have argued that Stellar Wind didn't trigger FISA? One possibility is a very strange argument offered by George Terwilliger, a former deputy attorney general under George Bush Sr. A 2006 article on the data mining program that appeared in the conservative *National Review* quotes Terwilliger as follows:

> "I think it's fair to say that the statutes contemplate the transfer of this generic type of data much more on a case-by-case rather than a wholesale basis," he says, meaning that the statutes call for a court order only in cases when the government is making a targeted request for information. But, he adds, "I don't see anything in the statute that forbids such a wholesale turnover."

Terwilliger also happens to be Alberto Gonzales' attorney and has been a prominent defender of the administration's surveillance policies. It seems entirely possible that the odd argument Terwilliger offered *National Review* might echo the justifications that his fellow Federalist Society member John Yoo developed while at OLC.

How might such an argument have worked? Here it's necessary to look a bit more closely at FISA's complex, overlapping definitions of "electronic surveillance." One way to trigger the definition is by "intentionally targeting" a "particular, known United States person"—no problem there if data was swept up indiscriminately and en masse. Two other prongs of the definition cover the live, realtime interception of communications contents as they're moving on a wire or through the air. There's precious little wiggle-room here, but it's conceivable that the kind of "metadata" gathered in the data mining program could have been obtained from telecom records or from databases of e-mails stored on servers.

Communications contents that aren't "in motion" on a wire or radio wave might still be covered under FISA's fourth catch-all definition of "electronic surveillance," which essentially applies to any other use of a surveillance device to collect communications. But *that* definition only applies in circumstances where someone enjoys a "reasonable expectation of privacy" in the information—the Fourth Amendment standard that, according to precedent, doesn't embrace non-content "metadata." (Though that still leaves those pesky e-mail subject lines.)

Even if we bought this slightly sophistic line of reasoning—it's hard to explain why FISA includes an explicit procedure for

obtaining pen register or trap and trace records if Congress believed such records weren't covered by the statutory definition—there would still be the problem of the Stored Communications Act. That's where Terwilliger's unorthodox reading might come in: The language of that law contemplates disclosure of records "pertaining to *a* subscriber to or customer" (emphasis added). Parse with tweezers and a microscope, and you might make the case that this should be read along the lines of the ban on "intentionally targeting" in FISA—a barrier to investigating some particular person, not on crunching the data in bulk.

Again, this is all speculation—the government is still fighting to block the release of any of the internal legal justifications of the NSA program written up by the OLC. But the legal theory laid out here at least seems to fit the known facts about the program, the law, and the handful of public statements made by attorneys in the know.

And if this *was* the theory on which the administration relied? One could charitably say it might pass for clever in a high school debate round. It would be deeply unsettling if it had passed for anything more in the halls of power.