



« [Hans Reiser Briefly Weeps; Explains Murder Books and Says Nina Dated KGB](#) | [Main](#) | [Audio: Helpful Hacker Gives a Security Lesson to Paris Hilton](#) »

## Whistle-Blower: Feds Have a Backdoor Into Wireless Carrier -- Congress Reacts

By Kevin Poulsen  March 06, 2008 | 8:15:00 PM Categories: [Spooks Gone Wild](#)

A U.S. government office in Quantico, Virginia, has direct, high-speed access to a major wireless carrier's systems, exposing customers' voice calls, data packets and physical movements to uncontrolled surveillance, according to a computer security consultant who says he worked for the carrier in late 2003.

"What I thought was alarming is how this carrier ended up essentially allowing a third party outside their organization to have unfettered access to their environment," Babak Pasdar, now CEO of New York-based Bat Blue told THREAT LEVEL. "I wanted to put some access controls around it; they vehemently denied it. And when I wanted to put some logging around it, they denied that."



Pasdar won't name the wireless carrier in question, but his claims are nearly identical to unsourced allegations made in a federal lawsuit filed in 2006 against four phone companies and the U.S. government for alleged privacy violations. That suit names Verizon Wireless as the culprit.

Pasdar has executed a seven-page affidavit for the nonprofit [Government Accountability Project](#) in Washington, which on Tuesday began circulating [the document](#) (.pdf), along with [talking points](#) (.doc), to congressional staffers hashing out a Republican proposal to grant retroactive legal immunity to phone companies who cooperated in the warrantless wiretapping of Americans.

According to his affidavit, Pasdar tumbled to the surveillance superhighway in September 2003, when he led a "Rapid Deployment" team hired to revamp security on the carrier's internal network. He noticed that the carrier's officials got squirrely when he asked about a mysterious "Quantico Circuit" -- a 45 megabit/second DS-3 line linking its most sensitive network to an unnamed third party.

Quantico, Virginia, is home to a Marine base. But perhaps more relevantly, it's also the center of the FBI's electronic surveillance operations.

"The circuit was tied to the organization's core network," Pasdar writes in his affidavit. "It had access to the billing system, text messaging, fraud detection, web site, and pretty much all the systems in the data center without apparent restrictions."

The [2006 lawsuit](#) (.pdf), which is suspended pending an appeals court ruling, describes a similar arrangement, naming Verizon.

Because the data center was a clearing house for all Verizon Wireless calls, the transmission line provided the Quantico recipient direct access to all content and all information concerning the origin and termination of telephone calls placed on the Verizon Wireless network as well as the actual content of calls.

The transmission line was unprotected by any firewall and would have enabled the recipient on the Quantico end to have unfettered access to Verizon Wireless customer records, data and information. Any customer databases, records and information could be downloaded from this center.

That doesn't mean Pasdar's affidavit confirms the claims in the lawsuit. He acknowledges speaking with the attorneys on that lawsuit before it was filed, so he may be the source in that complaint as well. But he insists he did not name Verizon or any other phone company to the lawyers.

"I don't know if I have a smoking gun, but I'm certainly fairly confident in what I saw and I'm convinced it was being leveraged in a less than forthright and upfront manner," Pasdar says.

Verizon spokesman Peter Thonis says he can't confirm or deny a Quantico arrangement, or comment on

whether Pasdar did contract work for the company.

"What you're talking about sounds as if it would be classified and involving national security, so I wouldn't be able to find out the facts," Thonis writes in an e-mail.

**Postscript:** In response to some of the comments here and elsewhere: No, it's not CALEA. CALEA requires phone companies to give the FBI real time access to call content and call detail information on specific targets when presented with a warrant. It does not oblige them to give the FBI or anyone else direct unmonitored access to switches, billing systems or databases.

For more on the FBI's CALEA network, check out [Ryan's article](#) on the subject from last year.

**Update:** Democratic leaders in the House are taking Pasdar's claims seriously. John Dingell, the chairman of the Energy and Commerce committee, wrote a [Dear Colleague letter](#) (.pdf) today, addressing the issue.

Mr. Pasdar's allegations are not new to the Committee on Energy and Commerce, but our attempts to verify and investigate them further have been blocked at every turn by the Administration. Moreover, the whistleblower's allegations echo those in an affidavit filed by Mark Klein, a retired AT&T technician, in the Electronic Frontier Foundation's lawsuit against AT&T. ...

Because legislators should not vote before they have sufficient facts, we continue to insist that all House Members be given access to the necessary information, including the relevant documents underlying this matter, to make an informed decision on their vote. After reviewing the documentation and these latest allegations, Members should be given adequate time to properly evaluate the separate question of retroactive immunity."

*Image: FBI.gov*

**See Also:**

- [Qwest CEO Not Alone in Alleging NSA Started Domestic Phone Record ...](#)
- [Senator Denies AT&T, Verizon Cash Bought Spying Immunity Vote](#)
- [Verizon and Government Seek Dismissal of Data-Mining Programs on ...](#)
- [Legally Questionable FBI Requests for Calling Circle Info More ...](#)
- [FBI Confirms Contracts with AT&T, Verizon and MCI](#)
- [AT&T, Verizon: We Obeyed FBI "Emergency" Requests - 739 of Them](#)
- [Verizon: Suing Us For Turning Over Customer Call Records Violates Our Free Speech Rights](#)

   186 points

 2003 diggs 

 Yahoo! Buzz

 Stumble

 ShareThis