wasn't Joe Average's conversations that the government was interested in. The wiretapping applied only to a small population: those persons believed to be communicating directly with terrorists. Such surveillance conducted without alerting the target, they argued, was a necessary weapon in the U.S. anti-terrorism arsenal. Or, as one retired judge put it: "You can't play poker with all up cards."

Following the press reports, the Bush administration vehemently defended the plan. Wiretaps without warrants were justified in President Bush's position of protecting the nation's security. Besides, Congress had given President Bush the authority just days after the horrific attacks of Sept. 11, 2001 to use "all necessary and appropriate military force" against terrorists. The Patriot Act had his back.

Debates ensued. Wouldn't such measures grease the already slippery slope of privacy erosion and, if left unchecked, become a sinister tool for prying into people's private lives? Lawsuits bubbled (one such class action suit filed Jan. 31, 2006 by the EFF against AT&T charges the telecom giant not only violated U.S. law but its customers' privacy in a "massive and illegal program to wiretap and data-mine Americans' communications."). Congressional hearings were scheduled. Suddenly everyone was questioning how the interpretation of laws governing what was permissible could be so unclear.

Surf and Its Turf

The subject of privacy in communication grew more flammable when weeks later, Internet giant Google was fighting the government about a subpoena the Mountain View, Calif.-based company had received in summer 2005. Google was asked to provide information from its database—randomly chosen Web site addresses—as well as the text of searches conducted over one-week period. The Department of Justice asked for the information so it could resuscitate its Child Online Protection Act (COPA) and demonstrate that federal laws are more effective than filtering software for protecting children.

What most disturbed many Internet users was that they knew how often they type in a query to Google. In almost a stream of consciousness, a word or phrase could be typed into Google's form, with the user unaware of what significance a particular search might have to a third party. Discussions raged on that the Internet, once perceived as an anonymous medium, was as translucent to the user's identity as two metal cans haphazardly strung together. From the pundits, it was all countered with the sentiment that rooting out terrorists and putting an end to child pornography could only be seen as a reasonable cause. If you've done nothing wrong, you don't have to worry about who is listening.

At approximately the same time, Google appeared in more headlines when it decided to enter the China market and hand over some control on what customers can view on search pages at the government's request. It all had the making of the "perfect storm" for privacy issues, according to Cindy Cohn, legal director at the civil liberties group Electronic Frontier Foundation.

Google's dilemma bled the privacy concerns of the voice network over to the data network, and mixed in the responsibilities of service providers and technology makers. Should customers expect such privacy when talking on their phones, when using the Net, or when thumbing with their Blackberry? Yes, say experts.

"If a third party has your info—mobile or landline—they should have obligations to keep that secret unless they get lawful process, and any violation of that is illegal," says Cohn.

But a service provider is at the mercy of lawful process. "The service providers have to do what they are asked for by the government," says telecom industry analyst Jeff Kagan. "So the bottom line is, with electronic and wireless communications we are fooling ourselves if we think it is private."

Complying with subpoenas is one thing, selling out to a third party interest is another. With security as a prominent concern, however, market experts say service providers promising shored-up networks, and strong business ethics not to divulge information unnecessarily could strike a market advantage.