"An assurance not to misuse the personal data by the service provider would be a better stand in the market, which is an inbound expectation of the general public," says Sathya Durga, analyst at market research firm Frost & Sullivan.

Google wasn't the first Internet player to hear the knock on the door from federal agents. Internet behemoths Yahoo, MSN, and America Online have also been requested, and have also complied, to supply search records from their databases. It's not that the Internet was overlooked by lawmakers. In 1994, Congress submitted guidelines to service providers in order to enable their networks to be more accessible to requests for information from law enforcement, and CALEA, or Communications Assistance for Law Enforcement Act, was born. There's also the Electronic Communications Privacy Act, which governs the interception and disclosure of communications, including stored communication.

It was a relief to Google when, back in March, a federal judge was leaning toward making off limits the search terms used by customers, but giving the Department of Justice access to some of Google's indexed Web sites, according to news reports. Google saw the move as justification of its own user privacy concerns regarding the DOJ's request.

"At a minimum, we've come a long way from the initial subpoena request, which was for billions of URLs and an entire week's worth of search queries," according to Nicole Wong, associate general counsel at Google. "When the government was asked to justify their demand they conceded that they needed much less." After negotiations, and before the judge's ruling, the government had reduced its initial numbers sought to 50,000 URLs and 5,000 search queries.

With the accelerated rate of progress of the technology, the art of surveillance detection might get much tougher down the road.

I Spy

Paul Herrmann, founder of eVestigations and a former head of global IT security at a major pharmaceutical company, knows firsthand the sophistication of surveillance tools. That's because eVestigations specializes in sniffing out such surveillance, be it in the form of an active bug that's detected by the energy it emits or a more stealth inactive one, which could require more specialized equipment such as X-ray devices and non-linear junction detectors (NLJD) to detect, he says. But with the accelerated rate of progress of the technology, the art of surveillance detection might get much tougher down the road.

"There's the possibility that in five years' time, it will be impossible to detect some of the government things that made it out to the commercial market," says Herrmann.

Technology on the mobile front is also giving cause for privacy debates. This spring, a GPS-enabled phone will be marketed in the U.S. as a means for parents to track the whereabouts of their child. Verizon Wireless is scheduled to launch the service, rumored to be dubbed Verizon Chaperone, this month with plans to roll out additional location-based offerings. The service will be available on Verizon's kid-oriented phone, tagged Migo.

Verizon Wireless' move will likely be followed by others in the wireless realm. That's because wireless operators years ago had to comply with federal mandates governing that the general location of a wireless phone could be pinpointed when a user was calling 911. The GPS, or global positioning system, chip embedded in mobile handsets was initially a means for fulfilling regulation. But with a niche—parents who want to know if