by Joshua Breitbart
Thursday, November 29, 2007 12:00 AM

Privacy advocates â€“ really, anyone who uses a phone or the Internet in the United States â€“ won an important victory before Thanksgiving when the Senate Judiciary Committee approved national intelligence legislation that did not provide retroactive immunity for the telephone companies that aided the Bush administration's illegal spying efforts. But the debate in the committee represented only one skirmish in the ongoing war over privacy in the digital age.

There is growing public awareness of the amount of data private corporations collect using tools like interactive Web sites, mobile wireless connections and global positioning systems, as well as remote computing through services like Google Docs and .Mac. Everywhere you look, the privacy issue rears its head: Some object to Mayor Michael Bloomberg's congestion pricing plan because it would allow the government to track who drives where and when.

At the heart of the issue is the question of whether our constitutional right to privacy will persist in an age of email and voicemail, or if it will fade along with personal letters and answering machines. Along with Congress, the courts are grappling with this question, deciding what standards the government must meet to gather information through different technologies. Their decisions have the potential to transform longstanding assumptions about privacy and limits on government.

The Legislative Battle

The legislation approved by the Judiciary Committee amends the Foreign Intelligence Surveillance Act to permit U.S. government wiretapping of all communications that cross or occur outside U.S. borders -- without a warrant. But President George W. Bush has threatened a veto unless the bill also grants immunity for the illegal wiretapping he already ordered of domestic communications. Any version of the bill, the president said, "must grant liability protection to companies who are facing multibillion-dollar lawsuits only because they are believed to have assisted in the efforts to defend our nation following the 9/11 attacks."

The Senate Intelligence Committee passed a version of the legislation that includes the immunity along with many other concessions to the Executive Branch. The House of Representative, though, already passed legislation without the immunity provision.

The Senate returns to the Capitol in early December to take up the Foreign Intelligence Surveillance Act. Senate Majority Leader Harry Reid has to choose which version of the bill to send to the Senate floor. Some observers say he is likely to choose the Intelligence Committee version, since it has bipartisan support. Opponents of immunity will try to make amendments to the bill on the floor or, failing that, promote the House version in the conference committee to

reconcile the different versions. If that fails, some senators have vowed to try to block the legislation.

With or without immunity, the resulting bill will allow for spying without warrants on people in the United States in some circumstances, eroding the privacy of our electronic communications.

The Legal Contest

The privacy issue is also being fought over in the courts. In a case currently before the 6th U.S. Circuit Court of Appeals, Warshak v. USA, the government asserts that anyone who stores their e-mail with a company like Yahoo! or Verizon -- which means the vast majority of us -- has given up any expectation that those e-mails will be private. The very fact that the host company can see the emails, the administration's reasoning goes, means the government should be able to search the messages without a warrant.

The case tests the constitutionality of the Stored Communications Act. Originally passed in 1986, it allows law enforcement to obtain e-mails, voicemails, and other information stored with a third party using a much weaker standard than the one protecting our paper letters and phone calls. Warshak is the first case asserting that people have a reasonable expectation of privacy when using e-mail.

On the one hand, it seems obvious that e-mails are private. As a group of Internet professors wrote in a friend of the court brief, a simple survey of the contents of e-mail communication shows that "we rely on the privacy of the medium. Society does not make us rely at our peril but rather accepts as reasonable our expectations of privacy in e-mail." And yet the widely reported government monitoring of e-mails itself erodes that expectation.

The court is getting set to hear the government's appeal of the lower court ruling that the Stored Communications Act violates the 4th Amendment. While the debate in Congress could tell us whether anyone will be held accountable for past unwarranted invasions of our private communications, Warshak v. USA could set the bar for privacy on the Internet going forward.

Patriotism or Profit?

The phone companies and their supporters argue that they should have immunity for the illegal wiretapping because company executives are patriots who acted in good faith to help law enforcement respond to the traumatic September 11 attacks. But recent revelations suggest the businesses were responding to the more base motivation of profit.

Joseph Nacchio, the former head of Qwest Communications, has asserted that the National Security Agency requested customer data as far back as February 27, 2001, almost nine months before September 11. When the agency admitted it had no legal order for the

request, he refused to comply. He claims the National Security Agency then retaliated by reneging on lucrative contracts. Nacchio was convicted of insider trading in April 2007; the loss of NSA revenue was part of his defense â€“ he claims they were the basis for the rosy forecasts he made while selling off some of his shares â€“ and he is appealing the conviction.

Comcast offers its employees a handbook to describe how to cooperate with requests from law enforcement. It includes a specific menu of fees to charge government: $1,000 to start an intercept, then $750 a month to maintain it. Call records are $150 for one batch per week, plus $50 for each additional delivery.

Many telephone companies have gone further, taking funding from the federal government to collect, store and analyze data on their customers, even sorting them into " communities of interest " profiles. The government could not collect such information without a subpoena, but the FBI argues that it is fine to outsource this surveillance to private companies to do it in anticipation of a subpoena.

The companies can feed any information or queries from law enforcement back into the system, mapping the social networks of anyone the government has under suspicion. They have regularly supplied information to law enforcement, not just in response to legitimate subpoenas but even to letters falsely claiming that subpoenas were on the way.

This is perhaps the biggest danger with data mining: Far from being a tool to collect information on known suspects, the collected information itself creates the suspects. So, if people create certain kinds of information about themselves â€“ legal, constitutionally protected information about who they associate with or where they travel â€“ that alone can make them suspicious in the eyes of their Internet service provider, their phone company and law enforcement.

An International Issue and a Local Issue

This debate is not limited to the United States. It is taking place wherever the Internet has taken root. The most well-known controversy might be the one involving Yahoo in China, where the Internet giant has helped the government track down dissident bloggers.

In England, law enforcement is trying for the first time to apply a section of the Regulation of Investigatory Powers Act , which forces people to participate in their own prosecution by handing over passwords to encrypted files on their own computer. The Crown Protective Service is apparently trying to use the act's mere existence to intimidate an animal rights activist into handing over her encryption key. In this scenario, simply possessing private, encrypted files becomes a crime or a cause for suspicion from law enforcement. (For more on the European Union's new data collection measures and the uproar they have caused, especially in Germany, see this previous column

).

In London, Bloomberg's inspiration for his congestion pricing plan, the system tracks the license plates of all cars entering and exiting the congestion zone. This has provided a foundation for a proposed "24-7 vehicle movement database" that would enable police to track all vehicle movement throughout the country â€“ 50 million trip a day, reportedly â€“ and store the records for two years. In response to these concerns, some have suggested ways to charge congestion pricing fees without tracking specific movements.

The recent strike by some New York City taxi drivers was over a related issue. The Taxi and Limousine Commission wants all cabs to install tracking devices in cabs that would tell the commission where the cars are at all times, regardless of whether the driver has a fare or is on personal time.

Whether it's the city government checking to see where a taxi driver is or the federal government reading your e-mail, the debate in both cases highlights the importance of preserving basic rights and protections in the face of potentially invasive technology. As we take advantage of new technologies and move more of our private documents and communications online, we need to strengthen our privacy protections, not weaken them.

Joshua Breitbart is policy director for People's Production House .