900 17th Street, N.W.
Suite 1100
Washington, DC 20006
Phone: 202.783.0070
Fax: 202.783.0534
Web: www.ccianet.org
Computer & Communications Industry Association

October 25, 2007

Via Facsimile

The Honorable Nancy Pelosi
U.S. House of Representatives
U.S. Capitol, H-232
Washington, D.C. 20515

Re: Proposed Immunity for Illegal Surveillance

Dear Speaker Pelosi:

The Protect America Act of 2007 made significant changes to the Foreign Intelligence Surveillance Act (FISA), and presents serious concerns about increased federal government acquisition and use of personal information about private American citizens. As you consider new legislation to address these concerns, while facilitating surveillance and tracking of targeted terrorists, I urge you to adopt safeguards against unnecessary intrusions into the lives of ordinary Americans by the U.S. Government.

Specifically, I write in support of the House Judiciary Committee's approach to retroactive immunity for telecommunications companies who may have supplied customer information and records without a warrant, subpoena or other official certification from the Justice Department, possibly in violation of FISA.

CCIA opposes the Administration's push for blanket immunity for telecommunications companies that have accommodated questionable or illegal government requests for wiretapping and surveillance. CCIA encourages you to reject broad immunity provisions in favor of a better balance between legitimate national security interests and basic Fourth Amendment privacy for U.S. citizens.

Telecommunications service providers have a civic responsibility to assist lawful surveillance requests by government and an obligation to protect the privacy of their customers. It is inadvisable for the trusted carriers of free speech by our customers, protected as it is by the First Amendment, to become ongoing de facto agents of government surveillance programs. Of course, where there is clear constitutional and legal authority to require specific cooperation we would expect companies to behave in accord with such requirements. But we believe companies also have a duty to their customers and to the integrity, freedom and openness of our networks.

The technology and communications industry in particular has a unique responsibility to ensure that networks remain free of unjust superintendence. Customers have a right to expect that their

real-time communications activities as well as their customer proprietary network information (CPNI) including call records, will not be disseminated or disclosed to third parties, including the government, without their knowledge. FISA procedures provide basic Fourth Amendment privacy protections. Commercial enterprises have the right to insist, as apparently one telephone company (Qwest) had done, that government requests for customer information be accompanied by appropriate legal authorization from a court or some official of the judicial branch of government.

Coerced industry surveillance will impair confidence in everyday telecommunications and online activities for business and personal use. If consumers cannot rely upon network operators to shield them from unjustified mining and seizure of their private information, electronic commerce and personal communications will be compromised.

In this age of ubiquitous digital communications and endless databases, American citizens deserve basic privacy protections against government misuse of their personal information, whether inadvertent or deliberate. Retroactive immunity breeds uncertainty that strains the resources of both national security officials and the telecommunications companies, who are reduced to guesswork about what unauthorized wiretapping or data searches might later be pardoned, due to circumstances of war or emergency. Further, prosecution of terrorists could be impaired by tainted, illegally obtained evidence. Finally, the reality that retroactive immunity for telecommunications network operators may not survive constitutional challenge is yet another reason for Congress to resist the immunity temptation.

Clearly, the civil suits that some have brought against their telecom providers alleging that certain companies turned over their personal information to a National Security Agency (NSA) eavesdropping program without a warrant partially motivate the Administration's requested immunity language. Nevertheless, those private plaintiffs are entitled to discovery of the underlying facts and their cases should be heard, even if national security concerns require that parts of such proceedings be closed to the public.

Accountability for illegal activity is essential to the rule of law. Presently, there has been no accountability and, save for revelations reported in today's Washington Post, there has been little disclosure regarding allegations of illegal surveillance. Without complete disclosure, no informed judgment can be made regarding potential legislative compromises about how to hold anyone accountable for alleged violations of the law.

I look forward to working with you on this important issue.

Sincerely,

Edward J. Black
President & CEO
Computer & Communications Industry Association

900 Seventeenth Street NW Suite 1100 Washington, DC 20006 Tel: 202.783.0070 Fax: 202.783.0534