



FENWICK & WEST LLP

# New Anti-Terrorism Law: Practical Issues for Internet Companies

ROGER M. GOLDEN AND DEVIN P. GENSCH

On October 26, 2001, the USA PATRIOT ACT (H.R. 3162) became law. This new law contains anti-terrorism authority that the Bush Administration requested of Congress following the tragic events of September 11. The law generally expands the investigatory powers of law enforcement agencies. The debate over whether this law represents a reasonable balance between the security needs of the nation and the civil/privacy rights of individuals is likely to continue as it becomes clearer how, and under what circumstances, law enforcement will invoke these new powers.

This voluminous law (nearly 400 pages in bill format) as well as related Congressional committee reports and floor debates are available online. See, e.g., <http://www.gpo.gov> (Government Printing Office) and <http://thomas.loc.gov> (Library of Congress). Major provisions of the law have been summarized in the press.

The new law could have significant consequences for Internet service providers (“ISPs”) and other providers of electronic and wireless services.

The law expands the authority of federal officials to intercept wire, oral and electronic communications in the case of terrorism as well as computer fraud and abuse. Subpoenas for records of electronic communications may demand, among other things, “telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)”. The civil Cable Act privacy provisions administered by the Federal Communications Commission are amended to reflect the expanded criminal law authority of the Government to compel disclosure of customer information pursuant to subpoena.

Moreover, in emergency life/death situations, the ISP or other provider of electronic or wireless services may voluntarily disclose otherwise private subscriber information if the “provider reasonably believes that an emergency

involving immediate danger of death or serious physical injury to any person justifies” such disclosure. The Government also has enhanced authority under the new law to obtain records of all numbers dialed from a particular phone line (“pen register”) and the originating phone numbers of all incoming calls on a particular phone line (“trap and trace”).

Finally, the Department of the Treasury is required within nine months to establish a “highly secure network” that will allow secure communications between financial institutions and the Government regarding “suspicious activities.”

Federal law enforcement officials will exercise the new investigatory authority with prior judicial approval, as required. At the same time, the Bush Administration is trying to coordinate all domestic intelligence activities under Homeland Security Czar Tom Ridge. The new statutory authority plus administrative consolidation of antiterrorism investigations within the Executive Branch are likely to result in more requests/demands for information about ISP and other wire and wireless service subscribers—particularly since the ongoing federal inquiry appears to indicate that the terrorists used communications technologies prior to September 11.

The recipients of increased official requests/demands for subscriber data may end up walking a narrow tightrope between their stated privacy policies and these new demands. The new law is not intended to eliminate underlying privacy statutes and case law but, clearly, the Executive and Legislative Branches have decided that in specified situations, certain information that could not have been obtained before September 11, 2001, from ISPs and other wire and wireless providers now can and must be obtained for reasons of national security. Companies and organizations who collect, store or transmit any personal information may wish to revisit their privacy procedures to ensure that law enforcement gets the information it needs while the privacy of consumers is protected in a manner consistent with stated policies.