

Progressive Policy Institute

Contact:

Rob Atkinson,

Vice President, PPI

Director, Technology and New Economy Project

Submission tailored for “Pen Register and Trap & Trace, e.g., section 101 of the Administration bill.”

New Dem Daily | DLC | September 24, 2001

Cyber Tools for Countering Terrorism

In the wake of the devastating terrorist attacks of September 11, the Bush Administration, led by Attorney General John Ashcroft, has proposed a package of antiterrorism measures (The Anti-Terrorism Act of 2001) aimed at providing law enforcement with a more effective set of tools than is currently available for the tricky job of ferreting out terrorists while their plots are still in the planning stages.

The proposed legislation addresses a number of anti-terrorism issues, including immigration, money laundering, criminal law, and electronic surveillance. Congressional leaders from both parties have signaled that the package will require significant work, and will probably move slowly, for the obvious and important reason that civil liberties concerns must be addressed.

But there's one section of the bill that strikes us as a common-sense modernization of law enforcement techniques, not an expansion of police powers or a threat to civil liberties. The electronic surveillance provisions essentially bring outdated wiretapping laws into the Information Age, reflecting the way people actually communicate and travel in the New Economy.

Law enforcement officials are currently required to obtain permission to place "Pen Register" and "Trap Orders" on a particular phone number -- for example, in a terrorist suspect's apartment -- in order to know what numbers the person is calling and what numbers are calling him. These days, of course, few suspects would ever use a single phone line. They'd more likely make calls from home, an office, a cell phone, or on the road, traveling from state to state. That raises another problem with the current law: law enforcement officials are now required to obtain a new order in each new jurisdiction a suspect may pass through in his travels. The new proposal would change that framework, allowing law enforcement to obtain a single order to monitor an individual, regardless of the phone he may use or the jurisdictions through which he may travel. And because electronic communication today can just as easily be a voice call or an email message, this provision sensibly extends Pen Register and Trap Orders to email messages (as long as the technology does not read the actual message, in which case a search warrant is rightly required).

The bill proposes a number of other reasonable modernizations. Like the nationwide order for Pen Register, the bill would allow law enforcement officials to use a legitimately obtained federal search warrant to read a suspect's email with the help of an

electronic service provider in any location. Current law limits the warrant to "property" located in the district of the issuing court. But a suspected terrorist might well be using an email service located across the country. That means investigators in one region have to work with law enforcement in other regions to get warrants to reach a service provider not located in the original district court region. Those time delays could fatally hamper the progress of an investigation.

The bill allows victims of computer trespassing (e.g., an Internet site that is being hacked) to authorize law enforcement officials to monitor trespassers on their computer systems. It would also allow law enforcement to access voice mail messages with only a search warrant, instead of a wiretap order that brings with it a higher level of court scrutiny. Currently, a copy of a fax or letter message only needs a search warrant.

There are a few provisions in the electronic surveillance section of the bill that at first glance give us cause for concern, such as allowing law enforcement to share information with other parts of the federal government without a court order. But by and large, this is not a rash, post-September 11 expansion of police powers; most of the proposals are a long-overdue updating of the law to reflect the way people, including terrorists, live and communicate today, using multiple channels of communications, from landlines to cell phones, pagers, Blackberries or laptops. Law enforcement officials will still have to go to a judge to make a case for search warrants and/or wiretaps.

But notwithstanding their modest, common sense nature, these proposals have raised howls from libertarians on both the Left and the Right. "It's almost McCarthyesque," Shari Steele, executive director and president of the left-leaning Electronic Frontier Foundation in San Francisco, told the Washington Post. The Center for Democracy and Technology goes further, calling for a rollback of existing law enforcement tools. Right wing, anti-government libertarians such as Rep. Bob Barr (R-GA) have weighed in hysterically as well.

In opposing common sense updating of our electronic surveillance laws, these groups rely on inflated scare tactics, conjuring up visions of Lincoln's suspension of habeas corpus during the Civil War and the internment of Japanese Americans after Pearl Harbor.

The simple truth is that the new proposals don't make it even a bit easier for law enforcement officials to classify anyone as a suspect subject to search warrants or wiretaps, much less authorize invasions of the privacy of law-abiding citizens. They simply keep the bad guys from evading detection by using modern means of communications outside the scope of an outdated law.

There will undoubtedly be plenty of bad ideas out there that genuinely do threaten privacy and civil liberties before the war on terrorism is over. True civil libertarians should focus on those, not on reforms that simply help those who protect our lives and liberties to find and prosecute terrorists.