

## **Ashcroft proposes vast new surveillance powers**

**by Kevin Poulsen**

**10 February 2003**

*SecurityFocus Online*

A sweeping new anti-terrorism bill drafted by the Justice Department would dramatically increase government electronic surveillance and data collection abilities, and impose the first-ever federal criminal penalties for using encryption in the U.S.

A draft of the Domestic Security Enhancement Act of 2003 dated January 9th was obtained by the non-partisan Center for Public Integrity and released Friday. The 120-page proposal would further expand many of the surveillance powers Congress granted federal law enforcement in the USA-PATRIOT Act in 2001, while increasing the secrecy surrounding some government functions.

The Justice Department hasn't released the proposal publicly, nor has it been formally submitted to lawmakers, but a legislative "control sheet" attached to the bill indicates that review copies were sent to Speaker of the House Dennis Hastert, and Vice President Richard Cheney last month. In a written statement Friday, a Justice Department spokesperson said it would be "premature to speculate on any future decisions, particularly ideas or proposals that are still being discussed at staff levels."

Civil liberties groups are already calling the bill "Patriot II".

"I just don't know where to start, it's just expanding everything," says Lee Tien, staff attorney at the Electronic Frontier Foundation. "When this hits the Hill there's going to be a lot more talk about what's going on, as opposed to the Patriot Act, where Congress just went on the government's say-so."

One provision in the bill would represent America's first domestic regulation of encryption, though it would apply only to those already attempting to commit a federal crime.

The new law against "Unlawful use of encryption" would establish prison terms for anyone who "knowingly and willfully uses encryption technology to conceal any incriminating communication" relating to a federal crime that they're committing, or attempting to commit. Offenders would face up to ten years in prison, in addition to the jail time the underlying crime carries, if any. A Justice Department analysis included with the proposal suggests that the illegal encrypting carry a mandatory minimum term of five years in prison.

Similar language has appeared in other government proposals dating back to the mid-1990's. But as encryption becomes more integrated into everyday Internet use, the idea of establishing a special punishment for using crypto borders on the ludicrous, says Tien. "As more and more Internet communications use encryption, it's going to be the default . . . It's like saying if you use a payphone you should go to jail."

Other provisions in the bill would:

- Allow a federal judge in one part of the country to issue a search warrant for a location in another part of the country in cases involving the suspected financing of terrorist organizations, attacks on critical infrastructure, or computer crime. The USA-PATRIOT Act allowed such inter-jurisdictional searches only in terrorism cases.
- Eliminate the requirement that federal agents issue a subpoena or obtain a court order to access someone's credit report. Under the bill, agents would only need to certify that they will use the information "in connection with their duties to enforce federal law" to secretly gain access to a consumer's credit profile.
- Expand grand jury secrecy rules to apply to witnesses, allowing prosecutors to order ordinary citizens not to divulge the existence of a grand jury investigation, or their own testimony, to anyone except an attorney. Current grand jury secrecy rules apply only to jurors, prosecutors and courtroom staff.
- Permit federal agents to monitor both voice and Internet communications from a target's Web-enabled cell phone, and to access the contents of the device's memory, with a single court order
- Expand the Foreign Intelligence Surveillance Act that governs U.S. spying on foreign nationals, and make it easy for agents to share foreign intelligence information with criminal investigators.

Many of the over 100 changes to federal law proposed in the bill don't involve the Internet. Among other things, the Domestic Security Enhancement Act would codify the Justice Department's position that the government doesn't have to identify detainees held in terrorism investigations unless they're charged with a crime. Another provision would expand a federal DNA databases of suspected terrorists. The bill would also strip some suspected American terrorists of their citizenship.

Copyright © SecurityFocus Online 2003  
Reprinted for Fair Use Only.