Your Privacy Is a Disappearing Act

LOS ANGELES TIMES

SUNDAY, DECEMBER 2, 2001

By BART KOSKO

We traded many civil liberties for increased police powers when President Bush signed the USA Patriot Act. Was it worth it? Is the potential increase in protection from terrorists worth the actual decrease in our privacy and other civil rights?

The answer depends on how the future unfolds. But there are good reasons for skepticism.

First, clever terrorists can outsmart the best efforts of law enforcement. The result is that many of the new laws may trade liberty for little or no security.

A telling example comes from a new finding in the Afghan war: The entire coalition war effort cannot crack the encrypted codes of Osama bin Laden, his officers and Taliban supporters. Intelligence sources say these enemy leaders can still communicate at will using sophisticated encryption devices that bury messages in seemingly harmless transmissions.

Such encryption software is freely available on the Internet—and all computers running for thousands of years could not crack it. We would need a breakthrough in "quantum computing," and none is on the horizon. That is why encryption remains central to Internet commerce and digital privacy.

Terrorists also can safely use "anonymous remailers" in cyberspace and multiple e-mail servers to hide their binary tracks. The grim prospect is that such digital anonymity may let future cyberterrorists act with impunity from anywhere in the world. Legislating away our e-privacy won't change that.

On the home front, Sen. Patrick Leahy (D-Vt.) supported the Patriot bill's sunset clauses—which set a four-year expiration date on some of the bill's provisions—because "the FBI generally doesn't pay any attention to oversight from Congress."

The FBI seized on the World Trade Center attacks to get surveillance powers that it has sought for years. That is why the Senate had so many proposed laws already in writing to vote on just hours after the bombing. For instance, the Patriot act eases search-warrant requirements to allow the FBI to monitor some Internet activity, such as phone numbers dialed and types of data transmitted. Agents need only "certify" to a judge that this non-content wiretap is "relevant" to a criminal investigation. (A content wiretap lets the FBI listen to a phone call or read an e-mail message, but it is much harder to get because the judge must see enough evidence to find probable cause.)

The FBI often uses non-content wiretaps to unleash its Carnivore e-mail sniffer. Carnivore snoops through the millions of e-mail and Web site bit packets that flow each second through Internet service providers, looking for a suspect's data. Can Carnivore look at a piece of a suspect's—or anyone's—e-mail and ignore its content? We don't know. We have to trust the FBI.

The Patriot act also creates "roving" wiretaps that let the FBI search any phone or data line that a suspect uses despite the 4th Amendment's requirement that a search warrant specifically describe the place to be searched. The act goes much further and achieves the old FBI goal of letting a local judge grant a nationwide wiretap.

Atty. Gen. John Ashcroft boasted that now his agents can "use a single court order to trace a communication even when it travels outside the judicial district in which the order was issued." That gives agents the incentive to shop for friendly judges likely to issue the warrants they want.

The new laws set the stage for even more anti-privacy measures in the event of future terrorist acts. A recent Harris Poll found that 68% of Americans favor a national ID card despite the dangers of pooling so much personal data in national and worldwide databases—and despite the ease with which terrorists could acquire false ID cards.

The same poll found that 86% of Americans favor government use of face-recognition software to detect terrorists. In January, city officials in Tampa used such software to match the faces in the Super Bowl crowd against its database of criminals. Yet simple disguises can still defeat the best face-recognition software. Accurate pattern recognition remains a distant goal.

These new laws may well prevent enough terrorism to justify their growing cost. Meanwhile, they have thrust us into a new age of digital surveillance that grows by gigabytes and sometimes terabytes with each linked database. Enjoy your privacy while it evaporates.

A digital spying net may or may not catch terrorists, but it will ensnare us.

Bart Kosko, the author of "Heaven in a Chip" (Random House, 2000), is on USC's electrical engineering faculty.