A Tool We Need to Stop the Next Airliner Plot

By Michael Chertoff
Tuesday, August 29, 2006; Page A15

Imagine that our troops in Afghanistan raided an al-Qaeda safe house and captured a computer containing the cellphone numbers of operatives in Europe. Wouldn't it be important to know whether one of those cellphone numbers was used to book a transatlantic flight? Unfortunately, today our ability to make that connection remains limited: Information that terrorists readily share with travel agents cannot easily be shared throughout the United States government. That needs to change.

Information sharing and intelligence gathering are some of our most important tools in the global war on terrorism. British authorities, in partnership with the United States and our allies, were able to disrupt the recent terrorist plot against passenger aircraft precisely because of timely, actionable intelligence, properly shared and acted upon before the terrorists could carry out their plans.

But despite the strong links we've forged with our European partners to protect our nations, we still remain handcuffed in our ability to use all available resources to identify threats and stop terrorists.

To defeat terrorists, we must limit their movement between countries and disable their worldwide networks by targeting our investigative resources. One technique practiced by the Department of Homeland Security and a number of foreign governments is the use of name-based information, such as passenger manifests and crew lists, to screen travelers coming to the United States before they get here. These manifests allow us to identify known persons of interest on watch lists and to act upon threats before they can reach our shores -- even, where possible, before they depart on their trip. But how do we thwart a terrorist who has not yet been identified?

One way is by using more of the detailed information collected by airlines and travel agencies when an individual books a flight.
These passenger name records contain information, such as travel itineraries and payment details, that can be analyzed in conjunction with current intelligence to identify high-risk travelers before they board planes.

If we learned anything from Sept. 11, 2001, it is that we need to be better at connecting the dots of terrorist-related information. After Sept. 11, we used credit card and telephone records to identify those linked with the hijackers. But wouldn't it be better to identify such connections before a hijacker boards a plane?

By comparing passenger name record (PNR) data and intelligence gathered on known terrorists -- such as cellphone numbers collected in Afghanistan -- we can identify unknown threats for additional screening and enhance our ability to assess risk. At the same time, that means we will spend less time with inconvenient screening of low-risk travelers.

The U.S. government has collected PNR data on travelers aboard international flights to the United States since the early 1990s. This information is of such value that after the Sept. 11 terrorist attacks, Congress mandated its continued collection. But in the past few years European privacy concerns have limited the ability of counterterrorism officials to gain broad access to data of this sort.

For example, under an agreement with the European Union, U.S. Customs and Border Protection receives this information regularly, but it cannot routinely share it with investigators in another DHS component, Immigration and Customs Enforcement, or with the FBI -- never mind with our allies in London. This information might yet identify associates of those arrested in the plot in Britain, but the rules blind us in routinely searching for that connection.

DHS has made a strong commitment to protect personal privacy while screening international travelers. We do not profile based on race or ethnicity, but we do assess potential threats through careful analysis of individual behavior. The DHS chief privacy officer has closely reviewed the PNR program to ensure that it meets standards of fair information practices and U.S. law. This includes providing a process through which travelers can seek redress if they feel their freedoms have been violated.

Protecting personal privacy is a part of responding to the post-Sept. 11 world, but it should not reflexively block us from developing new screening tools. Indeed, more data sharing leads to more precisely targeted screening, which actually improves privacy by reducing questioning and searches of innocent travelers.

All governments bear a responsibility to prevent terrorists from boarding aircraft, and information sharing is a critical way we can work together to limit terrorist mobility, screen for unknown threats and investigate terrorist cells. Smart screening -- including careful and responsive analysis of travel data -- will enhance security and privacy.

*The writer is U.S. secretary of homeland security.*