Spotlight

Wendy M. Grossman

> " A lot of the work in this field, as in many law enforcement fields, is making the right links between people and things

Peter Graham

Crossing Borders: The Right Side of Wrong?

Most nations consider travel data to be crucial to protecting national security. How that data is collected, stored, and secured however seems to be a closely guarded secret. Wendy M. Grossman investigates

Everyone's been through it: the wait after a long flight, the shuffle forward, and the brief delay while the border guard runs your passport through a scanner. Hopefully, you simply go on your way to your destination. But you leave behind a trail of data that began when you booked your ticket and created what's known as a Passenger Name Record (PNR), continued when you checked in, passed security, and boarded the plane, and culminates on arrival at the border.

What happens to PNR data has been widely discussed publicly in the wake of the EU's controversial decision to share that data with US authorities. What is much less well known is what happens to border data and how it is protected. The national border agencies – as well as Warsaw-based Frontex, the EU-wide border agency set up in 2005 – tend not to discuss it, though no data breaches stemming from border agencies have come to light.

"Most countries regard this kind of information around border security, watch lists, visas, etc., as some of the more sensitive data that we deal with", says Alex Bazin, head of biometrics for Fujitsu, which works for the UK Border Agency, among others. Both he and Peter Graham, an associate partner and border security expert for IBM, could not go into detail on any specific contract; their comments should not be taken as applying to any particular country.

Protecting National Security

Border data is sensitive both because people correctly view their travel data as exceptionally personal and because nations perceive this information as vital in protecting national security – not just for controlling immigration, but also for counter-terrorism and the fight against organized crime, and preventing money laundering, smuggling, and tax evasion.

A data breach, says Graham, might jeopardize all of that. "A lot of the work in this field, as in many law enforcement fields, is making the right links between people and things. Anybody who can access the system and disrupt those links can make

> **If you're a national, very little information is captured**

Peter Graham, IBM