AVIATION SECURITY INTERNATIONAL

www.asi-mag.com

AEROSPACE & SECURITY MEDIA
www.aerospace-media.com

THE GLOBAL JOURNAL OF AIRPORT & AIRLINE SECURITY

Threat Image Projection:

carrot or stick?

ALSO:

OPLAN BOJINKA

NAÏVE PASSENGER IDENTIFICATION

ARMING PILOTS

COMPARATIVE SECURITY

X-RAY OPERATOR PERFORMANCE

CREATIVE CONCEALMENTS

EILAT'S NEW INTERNATIONAL AIRPORT

SHARING DATA, SHARING RESOURCES:

MOVING FROM 'COULD' TO 'SHOULD'

by Philip Baum

Ordered a pizza by telephone recently?

"Hello! Giulia's Pizza?" You expect the answer to be a 'yes', but instead it's, "No sir. It's Google's Pizza." You ask if it's a wrong number, but the response is, "No sir, Google bought Giulia's Pizza. Do you want your usual?"

Your usual? How do they know what you normally order? So you ask if they know you. "According to our caller ID data, over the last 12 months, you have ordered 11 thick crust pizzas, each with spicy beef, extra cheese, mushrooms and cream, together with a side order of chocolate cookies and a vanilla milkshake." However, the woman continues, "May I suggest to you that this time you try our vegetarian pizza with leeks, spinach, onion, courgette and aubergine?"

"What?", you exclaim. "I hate vegetables". "But sir, your cholesterol level is not good," she retorts. "How do you know?" you ask.

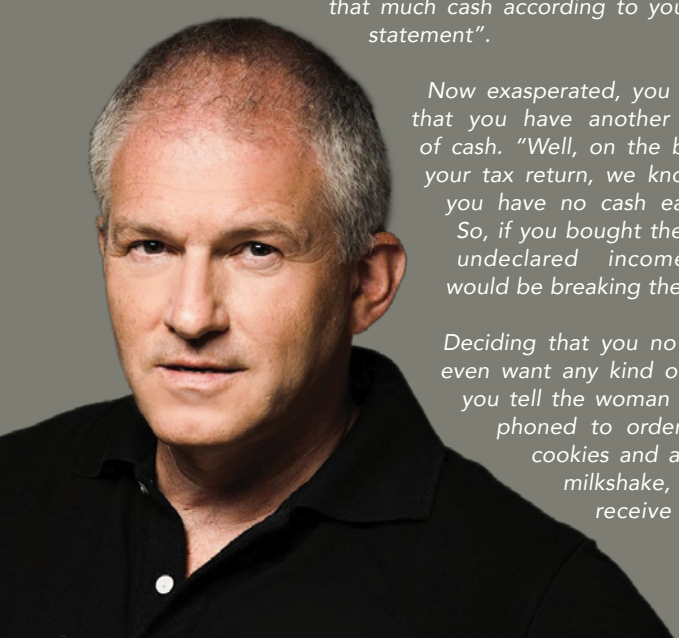
"We cross-checked the number of your landline with your name, through the subscribers guide and we now have the results of your blood tests for the last five years.". Angrily you assert that, "I want my usual pizza. I already take statins to address my cholesterol problems."

"Excuse me, but we know that you have not been taking your statins regularly. Four months ago, you purchased a box with 28 cholesterol tablets at your local chemist and you have not been back there since. You also have not obtained a new prescription."

"I bought more from another chemist over the counter."

"Really sir? It's not showing on your credit card statement"

"I paid in cash," you exclaim. "But you have not withdrawn that much cash according to your bank statement".



Now exasperated, you explain that you have another source of cash. "Well, on the basis of your tax return, we know that you have no cash earnings. So, if you bought them with undeclared income you would be breaking the law."

Deciding that you no longer even want any kind of pizza, you tell the woman that, "I phoned to order pizza, cookies and a vanilla milkshake, not to receive either dietary or financial advice. I'm sick of Google, Facebook, Twitter and all other forms of social media. This is the final straw. I'm going overseas to an island without any internet or cable TV and where there is no mobile phone coverage and nobody to watch me or spy on me."

"I am afraid that's not happening sir. Your passport expired three weeks ago!"

Of course, this is slightly stretching the extent to which our every transaction is being monitored. Many readers will, however, be familiar with the kind of product marketing tactics which display an uncomfortable familiarity with our browsing history, product purchases, entertainment preferences and even political leanings. Big data shared, either intentionally or inadvertently, is certainly shaping our lives.

"...in the hierarchy, or even caste system, of security agencies, the Police, Immigration and Customs are top dogs and those who are actually fulfilling the screening tasks are clearly bottom of the security pile and are often treated with disdain..."

Granted the commercial benefits that are clearly being exploited nationally and internationally, questions remain as to why within a single airport we seem incapable of utilising the available data effectively to enhance the security of our industry. Why is it still the case that our checkpoint screeners operate blindly, with no knowledge as to how or where passengers bought their tickets, when they last travelled, where they live or even, in most cases, where they are even travelling to? And yet we expect them to make decisions which, if incorrect, can have catastrophic consequences which go way beyond the potential loss of life on any one aircraft.

Data protection concerns and political correctness may be the justification for the controls which exist on the transfer of personal information between industry stakeholders, yet what is completely unacceptable is the failure to share security resources between agencies operating at airports. There are far too many reports from around the globe of states where agencies maintain the silo mentality, where ego gets in the way of actioning intelligence and, worse still, preventing true security being achievable. In the hierarchy, or even caste system, of security agencies, the Police, Immigration and Customs are top dogs and those who are actually fulfilling the screening tasks are clearly bottom of the security pile and are often treated with disdain. They can be overruled by every other agency, despite the fact that many of the officers deployed by the 'superior' agencies often have very limited, or even zero, aviation security experience.

Picture the following scenario. A passenger causes extreme concern at a security checkpoint. The archway metal detector alarms. The security guard asks the passenger to

remove their belt and shoes and go through the archway a second time. Another alarm. The passenger is then screened using millimetre wave technology. No alarm, but concern remains. The screening supervisor wants the passenger screened by a more advanced technology and knows that Customs have a transmission X-ray system for use in the identification of internally concealed narcotics. In your airport, what are the chances of permission being granted for such an inspection?

There are a broad range of security technologies available for use, and many more that could be deployed for the benefit of a range of security agencies. The stumbling block is often cited as being that of finance, but often it is also down to protectionism where one can sense that a fear exists of one agency detecting an illegal act which another agency should have identified.

This is not the case in every state. Many do foster cooperation. Often, however, that is in principle only and, for those operating at the coalface, the reality is somewhat more challenging.

Finance is actually rarely a genuine impediment to progress. If one were to calculate the actual cost of a single air force interception of a commercial aircraft which has been the subject of a bomb hoax or has an unruly passenger on board, it would dwarf the cost of purchasing some of the most sensitive and advanced detection technologies. The difference is simply that the cost of the interception comes out of an almost limitless defence budget whereas the purchase of a screening technology has to be fought for, often for years. And by which agency? And out of which cost centre?

A utopian view of the aviation security regime would, arguably, see a host of new technologies deployed. Explosive detection technologies for baggage and cargo screening could be integrated into aircraft holds or, at least, utilised during the loading process to further mitigate the insider threat. Passenger data, available to immigration officials, could be better utilised in the passenger screening process without compromising personal privacy. The idea of screening passengers on the move, mooted decades ago, is entirely achievable today and is used by customs and quarantine agencies. Facial recognition solutions could be used far more extensively to identify known criminals and those on government watchlists. Advanced perimeter intrusion detection systems could significantly address the scourge of airside trespassing for either criminal gain or in an attempt to stowaway on board aircraft. Could is not good enough…

> "…move from a 'could do culture' to a 'will do attitude'. And that can be achieved by cooperation. Breaking down silos. Reining in inflated egos. Sharing resources…"

We need to move from a 'could do culture' to a 'will do attitude'. And that can only be achieved by cooperation. Breaking down silos. Reining in inflated egos. Sharing resources. And above all, working towards our common goals.

In most of our personal and business transactions there is now a greater sharing of information and resources than we would ideally wish for. But it works. To successfully protect our airports, aircraft, passengers and employees, we need to learn to move beyond striving to comply with standards and seek to excel. We cannot do that without functioning as a team and enhancing security in the same way that commercial operations generate increased sales. That means recognising that all security challenges are inter-related and, therefore, warrant unbridled interconnectivity.