30 December 2009

In August of 2002 I endured a personal challenge. At the time, I was sitting on a bar stool at a friend's house in my Iowa home town listening to a classmate prattle on about 9/11 and all of America's associated failings and shortcomings. He was a friend of mine, and we'd spent time with him, his wife and kids, but that didn't change the fact that he knew just about zero regarding the subjects he was sanctimoniously preaching about. My challenge was that I did—in detail. But I couldn't talk about it.

Consequently, I had to sit there until I couldn't take it any longer. Wallowing in my lack of available candor, I resorted to an alcohol fueled, not-so-brilliant rejoinder along the lines of "You're full it." Only I didn't say "it."

We are likely to see a similar blast of ill-informed, half-informed and outright ignorant rants about America's failings and shortcomings related to this year's Christmas Day bomber Umar Farouk Abdulmutallab's attempt to blow up a U.S. bound passenger jet. Just as with my classmate's ill-informed passion without supporting knowledge and understanding, these rants, attacks and assertions will likely do more harm than good and simply degenerate into yet more useless partisan sewage.

The rants will center on the processes that allowed a man whose own father had reported as a radicalized Islamist to buy a ticket with cash and check in with only a backpack and yet not receive secondary pre-boarding security screening. The assertions will center on the databases where the information about terrorists is stored and made available to all relevant U.S. security agencies and organizations. The challenge is that the failures in this case are not about process or technology, they are about humans and human behavior.

A month after 9/11, I wrote in my industry magazine column a call to action to create the information systems that can (and, when properly implemented, do) identify terrorists within the available data sets in our society. That column, "We Can," became a rallying cry in the data management industry, and was used as a template and an inspiration for many systems that followed, including some involved in this situation.

A year later I wrote a follow-up column titled "They Can't," which mourned the year lost to U.S. agency bureaucratic infighting, turf wars and the agencies and departments willful ignoring of simple, basic lessons that the data professionals in my industry had learned long before. Sadly, some of those basic lessons cited in that 2003 column are still at work today, six years later, in this attempted bombing.

In particular, two examples still ring true today. First, as in John Poindexter's disastrous Total Information Access (TIA) initiative, there is very little demonstrated understanding of how the world works in the way today's systems are implemented. Second, as in Illinois Senator Dick Durbin's comment, "It's about protecting their turf and their jobs. That runs 180 degrees counter to what this nation needs at this moment."

Here's how it played out this time. In our fishbowl of American society, people buy airline tickets with credit or debit cards. Anyone walking up to a counter to buy a $2,831 ticket with cash, as the bomber did, is immediately suspect, and the cash purchase is grounds to flag the reservation, ticket and boarding pass for additional security screening, including interviews and physical inspection. However, in the developing world, including Accra, Ghana, where Abdulmutallab bought his ticket on 16 December, cash is king for all purchases. People in the developing world, especially Africa, do not commonly carry credit cards. For instance, Nigeria had about 600,000 credit and debit cards for its 149,000,000 people in 2007. Consequently, airline tickets in the developing world, including those to travel to the United States, are typically purchased with cash.

Where do people come from who attempt to, or succeed, in blowing up airplanes? The overwhelming majority originate in the developing world. However, the U.S. system for flagging tickets purchased with cash does not require foreign airlines, including those serving the developing world, to provide that data. While the U.S. does require all airlines to transmit in advance a complete passenger manifest of the names of everyone on every inbound flight to the U.S., the agencies involved ignore a datapoint, cash purchase, that is a key differentiator to separate regular travelers, such as business people or frequent leisure travelers, from those who are not.

Is this because the people involved with the systems have no exposure to or experience in the outside world? Hardly. The director of the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC), Timothy Healy, is a former U.S. Marine pilot. The principal deputy director of TSC is Don Torrence, who served for 24 years in the Army in a wide variety of intelligence roles. The deputy director is Zandra Flemister, who spent more than 30 years in State Department posts all over the world, including a recent posting in Islamabad, Pakistan.

The TSC's vision is "To be the global authority for watchlisting and identifying known and suspected terrorists." Their mission is "To consolidate and coordinate the U.S. Government's approach to terrorism screening and facilitate the sharing of terrorism information that protects the Nation and our foreign partners while safeguarding civil liberties." How they do it is: "The Terrorist Screening Center (TSC) maintains a consolidated database of the names and other identifying information for all known or suspected terrorists, known as the Terrorist Screening Database (TSDB)."

On their web site, they state that: "The TSC supports federal, state, local, territorial, and tribal law enforcement agencies and some foreign governments that conduct terrorist screening by making the TSDB information available to them for screening purposes. TSC's 24-hour call center also supports agencies' terrorist screening processes by determining whether the person being screened is an identity match to the TSDB. TSC supports terrorism screening at agencies like the State Department (passport and visa applications), the Bureau of Customs and Border Protection (border crossings and international flights), the Bureau of Citizenship and Immigration Services (immigration and citizenship applications), and the Transportation Security Administration (domestic flights). The TSC has also made Terrorist Identities Information accessible through the National Crime Information Center (NCIC) system to law enforcement officers, including 870,000 state and local officers nationwide, adding those resources to the fight against terrorism."

So there you have it, the single, unified, "go to" source for terrorist identity information for all relevant agencies, departments and law enforcement organizations in the United States, as well as some foreign governments: the TSC's Terrorist Screening Database (TSDB).

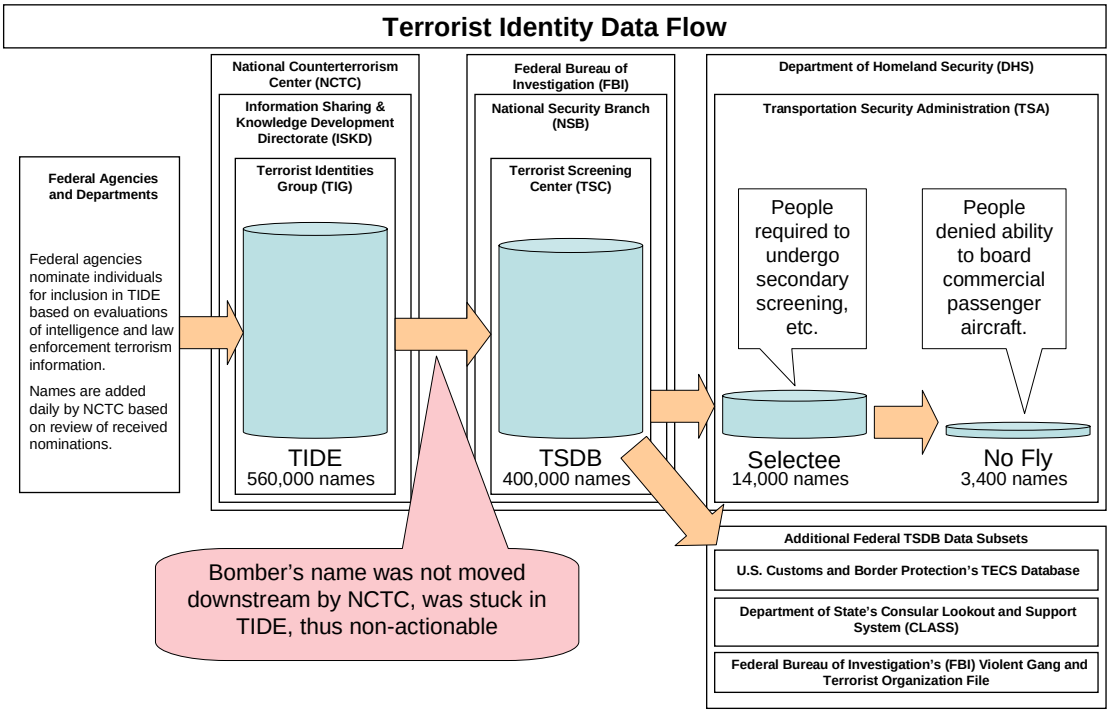
That single, unified, "go to" source is managed by people who have extensive, first-hand knowledge of how the real world works. And yet the system to determine if people boarding planes bound for the United States should receive secondary screening and inspection lacks two simple rules, two simple logic tests. Test one, does this person exist in the TSDB data, yes or no. Test two, does this ticket have characteristics that make it unusual, such as a cash purchase, no checked in bags or a one way ticket, yes or no. The first of these two simple logic tests would have flagged the bomber as soon as he purchased his ticket. The second would have flagged him when he showed up to check in for the flight.

Clearly, the people running the TSC program know enough about how the real world works to know those two simple tests can and should be applied against their data. Why isn't it applied when it makes so much common sense to do so?

The answer is related to the second issue: "It's about protecting their turf and their jobs."

The reason why the bomber could walk onto that plane, the reason why his name did not trigger a response in the FBI's TSDB terrorist database, the reason why he did not merit additional security screening by the systems based on the Department of Homeland Security (DHS) Transportation Security Administration's (TSA) Selectee or No Fly databases that are derived from the TSDB, is that *he didn't exist* in any of those databases. When he walked onto Northwest Flight 253 the bomber's name, his database record, only existed in the Terrorist Identities Datamart Environment (TIDE) created and maintained by the Terrorist Identities Group (TIG) located in the Information Sharing and Knowledge Development Directorate (ISKD) of the National Counterterrorism Center (NCTC).

If you were keeping count, there were ten distinct U.S. government fiefdoms in the preceding paragraph, each with its own stakeholders, bureaucracies, budgets, teams, managers and directors. Each fiefdom is competing for its own recognition, its own advancement, its own expansion, and, most importantly, its own budget. And remember, that paragraph only addressed one single set of data. Take that paragraph and multiply it by the hundreds to thousands of data sets involved in terrorism and you start to get an idea of the challenges involved around "It's about protecting their turf and their jobs."



In this case, even though the bomber's father had met with the American Embassy to inform them of his son's activities and indoctrination, and the relevant agencies, including the CIA, FBI, DHS and the Department of State, met to discuss the situation, the bomber's identity never made it past the TIDE data set into the TSBD data set.

No one paid any attention to Umar Farouk Abdulmutallab as he checked in with no luggage or boarded the plane with a bomb between his legs because his name was still stuck upstream, never flowing down the chain into the actionable data sets that the systems use to ring alarm bells, get people searched and prevent them from flying.

Why was it stuck? It was stuck upstream due to human decisions. The process for the first step in the data flow, from the TIDE data set to the actionable TSDB data set is: "Every evening, TIDE analysts export a sensitive but unclassified subset of the data containing the terrorist identifiers to

the FBI's Terrorist Screening Center (TSC) for use in the [United States Government's] USG's consolidated watchlist. This consolidated watchlist, which is a critical tool for homeland security, supports screening processes to detect and interdict known and suspected terrorists at home and abroad—for example, the Transportation Security Administration's "No Fly" list and the Department of State's visa database, among others."

Umar Farouk Abdulmutallab's name was in the TIDE data set, placed there by field agents in the U.S. embassy in Nigeria. The agencies and department involved, the NCTC, CIA, FBI, DHS and the Department of State, did not see fit to move his record downstream into the actionable data in the TSDB and other subsets.

Why didn't they move it? Because they were trapped within rules of human behavior related to information.

The challenge the NCTC, CIA, FBI, DHS and Department of State failed to overcome is a primary rule of information everywhere, whether it's information you have or your work team has or your company has or your country has—that rule is: My information is, by default, more accurate and reliable than anybody else's information. A fundamental human behavior attaches primacy of accuracy and relevance to any information that you, your team or your tribe possesses. Others' information is always suspect, if for no other reason, that it's not your information.

This rule of human behavior as it relates to information leads to individuals and groups forming a "silo" of information that is simultaneously jealously guarded from others to protect it from contamination and relied upon for most, if not all, decision making. It is commonly the primary, if not sole, source of information since any other source of information is, by its very nature, inferior.

Your information is better because it came from your information feeds (sources) (which you trust, again, largely because they are yours rather than due to any objective measure). Your information is better because the only modifications to it are the ones you deem worthy and correct (again, largely because they are yours rather than due to any objective measure).

In addition, your information is better because it is exclusive and unique because you control access to it. You only share it with selected individuals, groups, tribes and organizations who you have decided pose no threat to you and your stakeholders. Consequently, your information is never subjected to questioning, critical thinking or objective review.

In the case of the Christmas bomber, both of these factors, the primacy of self-sourced information and the controlled access to information, played a part.

Regarding primacy of self-sourced information, according to a U.S. administration official, there was "insufficient derogatory information available" about the bomber to move his database record downstream from TIDE for inclusion in the single, unified, "go to" source for terrorist identity information for all relevant agencies, departments and law enforcement organizations in the United States, as well as some foreign governments: the FBI's TSDB.

The reason they thought there was insufficient derogatory information available is that the initial tip that introduced the U.S. government to the bomber came from the bomber's father. And, if there is one ironclad rule in the agencies and departments of the U.S. government it is that while other agencies' information is, without exception, inferior to our agency's information, information provided by citizens—mere mortals—is, without exception, useless. The bomber's father, Umaru Abdulmutallab, a respected retired banker, was unaware that reporting his son to the United States intelligence community would draw a collective shrug.

The reason why the bomber, Umar Farouk Abdulmutallab, had an active multiple-entry U.S. visa was because the Department of State didn't consider the information provided by his father, a citizen—an outsider, was worthy of their time, attention and energy—in short: their work—to revoke it. The reason why the bomber, Umar Farouk Abdulmutallab, did not appear in the FBI's TSDB database or the TSA's Selectee or No Fly databases was because they did not consider information provided by his father, a citizen—an outsider, was worthy of their time, attention and energy—in short: their work—to include the bomber's record.

The second factor, controlled access to information, was manifested by multiple U.S. agencies who had, but did not effectively share, information about the bomber's movements, his plans, and the plans of leaders of a branch of Al Qaeda in Yemen who were talking about "a Nigerian" being prepared for a terrorist attack. This jealous guarding of information is particularly galling to U.S. taxpayers who have invested billions of dollars since 9/11 to prevent this specific thing from happening. Ironically, both the NCTC's TIDE and the FBI's TSDB claim they exist and are funded as a direct result of the 9/11 commission's recommendation to end information hoarding and facilitate information sharing.

Unfortunately for the commissioners and the American taxpayer, you can build as many multi-billion dollar technology systems as you want, but you'll never overcome the human desire to prevent others from accessing internal, captive (siloed) information. This is especially true if others might use that information to advance their agenda (read: increase their budget at the information holder's expense), gain publicity or elevate their stature above that of the information holder's. In this contest, bureaucratic organization and tribal priorities trump national priorities every time.

Even after all the lessons learned from 9/11, even after all the billions of dollars spent, even after all the new and reorganized bureaucracies that have been created, the people we depend on to provide our security consciously chose to ignore information because it was provided by a mere citizen and also consciously chose to not share what self-sourced information they had in hand.

Viewed objectively from the outside looking in, these decisions seem ridiculous. Viewed from inside any one of the agency and department fiefdoms involved, they seem logical and essential to "the only valid information is our information" and "we do not share our information" characteristics of human behavior.

When you combine the lack of applying first hand knowledge of how the world actually works with active resistance to non-self-sanctified information with a deeply imbedded loathing to sharing information, you end up exactly where we are right now—relying on the ineptitude of terrorists and the courage of passengers to keep the planes in the sky.

Seven years after my August 2002 personal challenge, I now endure another. Every day brings a new round of finger pointing between governments, parties, agencies and departments attempting to deflect responsibility for letting a known suspect with known Islamist beliefs with known co-location to known Islamist terrorist cells with known ticket and check-in terrorist characteristics to blithely board a jet bound for the U.S. with a bomb strapped to his crotch.

Eight years ago I wrote that my peers, the data professionals, had the experience, capabilities and technologies required to connect the dots of terrorism.

Seven years ago I wrote that the agencies and departments of the U.S. government, due to willful ignorance and blinding self-interest, could not.

They still can't.

****

Distribution and Excerpts:

- This document is available here: http://www.hackneys.com/docs/theystillcant.pdf
- This document may be distributed in its entire, unaltered, unedited, original form.
- Excerpts may be made and distributed if attributed to this author, Douglas Hackney, document and source.

Notes:

- All information included is public source / knowledge
- My inability to discuss what I knew in August 2002 was and is due to confidentiality agreements, non-disclosure agreements, contracts and organization/entity policies
- While positioning citizens and the information they provide as useless may seem a harsh indictment of federal agencies, I know this for a fact based on our own experiences. I can state unequivocally that if you tell the FBI, DHS, Drug Enforcement Administration (DEA) and U.S. Customs about a multi-convicted felon who is committing a crime, they will ignore you.

****

Sources:

- Central Intelligence Agency (CIA)
- Federal Bureau of Investigation (FBI)
- Department of Homeland Security (DHS)
- U.S. Department of State
- U.S. National Counterterrorism Center (NCTC)
- U.S. Government Accountability Office
- Wall Street Journal
- New York Times
- San Francisco Chronicle
- Associated Press
- Reuters
- Ideaion News Press
- Creditcards.com

