A wasted opportunity in war on terror

By Hiawatha Bray  |  August 15, 2005

Did US military spies finger Mohammed Atta as an Al Qaeda terrorist a year before the Sept. 11 attacks? A US congressman says yes; leaders of the bipartisan 9/11 investigating commission say no.

But the controversy should remind us of one indisputable fact: A technology that may have helped spot Atta and other terrorists is being suppressed by Congress, for no particularly good reason.

That technology is "data mining," the use of sophisticated software and powerful computers to spot patterns of activity hidden in vast amounts of apparently random data. It's used routinely by businesses seeking new ways to empty our wallets.

When you swipe one of those discount cards at the supermarket, you're letting the retailer make a record of everything you buy. Thus the store develops a profile of its customers' tastes and buying habits. Mining this data can reveal patterns that would otherwise go unnoticed.

For instance, purchases of bottled water may increase whenever there's a sale on sirloin steak. Data mining uncovers thousands of these nearly invisible correlations, and marketing wizards use the results to maximize the store's profits.

But data mining can also be used to spot interesting patterns in other kinds of data. Just by crunching credit card numbers, you could find out that there's some guy in Chicago who's been buying an awful lot of fertilizer -- the kind that can be turned into truck bombs. Or someone in New York who does a lot of travel to exotic foreign locales, and who also signs up for courses on how to fly jumbo jets.

According to The New York Times, a secret Pentagon program called Able Danger used data-mining technology to determine that Atta and three of his 9/11 buddies were probably members of an Al Qaeda murder cell on US soil. If true, it's an impressive piece of detective work. And the data miners might be capable of even more remarkable feats, if only our government hadn't wasted the past two years.

In 2003, members of Congress of both parties shut down an experimental military research program called Terrorism Information Awareness. Originally known as Total Information Awareness, or TIA, the program was run by Admiral John Poindexter, best known for his
felony conviction -- later overturned -- in the Iran-Contra scandal.

TIA was an experimental effort run by the same military research agency that led the development of the Internet. This time, the goal was to develop technologies that would search hundreds of government and commercial databases, in search of patterns that might indicate criminal or terrorist activity.

Note the word "experimental." TIA was nowhere near ready for actual use. Poindexter and company wanted to use made-up data that resembled the stuff in real-world databases. The data would be seeded with subtle hints of suspicious activity, based on actual terrorism incidents. TIA would try to develop technologies that would spot the patterns and sound the alarm.

But the mere idea of TIA horrified civil libertarians right across the political spectrum. Former New York Times columnist William Safire led the way, claiming that Poindexter wanted to create dossiers on every American -- an absurdly inaccurate description of the project. But no matter. The resulting firestorm led to the shutdown of the project and to Poindexter's resignation.

These days, Poindexter spends his days sailing on Chesapeake Bay. He doubts that data mining alone could have rolled up the 9/11 terror network.

"It was only after the fact that the significance of this particular group was seen as important," he said.

Still, Poindexter believes that if Able Danger information had been shared with other law enforcement entities, it might have made a difference.

"There may very well have been other evidence that would have made the group stand out," he said. The advanced techniques he'd tried to develop might have enabled even better information analysis, and better sharing of data between law enforcement agencies.

"I do think that cancellation of the TIA programs did weaken the nation's security," said Poindexter.

Maybe he exaggerates. Some computer industry experts doubt that TIA could ever have worked.

"I thought it was a harebrained scheme," said Richard Smith, a computer security expert and former head of the Privacy Foundation. Smith doubts press reports that the Able Danger team used data mining to spot Atta.

"It was simple spy work that identified these people," he said.

Smith is biased, in an admirable way. He's horrified, with good reason, by TIA's potential to invade our privacy. But it's scarcely rational to ban the program outright, like outlawing telephones because they can be tapped. Instead, programs like TIA should have continued, on an experimental basis. Its developers were already testing ways to build privacy into this system. For instance, you can analyze credit card purchases without knowing the names of the cardholders.

Meanwhile, Congress could have calmed down and set sensible restrictions on the system's real-world use. Suppose TIA's anonymous credit card analysis spots something hinky, and the cops want a name and address. We might let them have the info, but only
if a federal judge agrees.

By now, TIA researchers would have two more years of know-how under their belts. And lawmakers could have crafted strong but flexible statutes to prevent abuses. Instead, federal data-mining projects continue, but they're buried inside the "black" budgets of our various spy agencies. Here it will be even harder to ride herd on the projects -- and harder to ensure evidence of an impending attack is shared with cops on the front lines.

It's possible -- likely, even -- that another Mohammed Atta is already in place, rehearsing for the next nightmare. Last week's report suggests that smart, aggressive use of computer technology could help us spot him before it's too late.

Does anybody care?

*Hiawatha Bray can be reached at bray@globe.com.*

© Copyright 2005 Globe Newspaper Company.