Few subjects raise the hackles of civil libertarians and ordinary citizens alike more than profiling, the process by which institutions target people based on traits such as race, national origin, ethnicity, psychological makeup, behavior, and past actions.

My cousin Jake McNicholas, a retired New York City police detective, was roundly criticized, for instance, after he wrote a recent newspaper column describing how he often had "used a person's race to initiate investigations and make subsequent arrests." The tools of his trade? Mere observation: following white guys driving cars with New Jersey plates slowly through predominantly black neighborhoods, in many cases looking for drugs. Even when profiling works and is done without malice, the fear of abuse is a powerful undercurrent.

While profiling is most often associated with cops, everyone from insurance companies to bank lenders to e-commerce sites to fast-food restaurants engage in the practice. The tools of their trade? Data mining and analytics software, tracking and monitoring technology, and other kinds of IT. Done right, these tools help companies identify the best potential customers or help them give customers precisely what they want when they want it. Done wrong, they invade privacy and can introduce serious mistakes. And there's a sea of gray between the right and wrong.

The police and intelligence communities are also big IT users, with mixed success and public backing. One of IBM's chief scientists, Jeff Jonas, has warned against using data mining to root out terrorists in the broad population. Jonas has argued that data mining is useful in identifying shopping habits and financial fraud, where results don't have to be pinpoint accurate, but not in identifying a few potential terrorists among hundreds of millions of people. Such analyses register false positives more than 90% of the time, Jonas argued in a report written a few years ago with the Cato Institute's Jim Harper, rendering analytics for anti-terrorism "useless and potentially harmful." Data mining has had success in law enforcement on a far more limited scale, like with deploying more police to areas where data analysis has determined an increased probability of a crime occurring.

I got to thinking more about IT-based profiling after reading a fascinating column by my colleague Alex Wolfe on a dozen recent IBM patent applications for airport security technology that purports to analyze characteristics such as age, type of clothing, facial expressions, even smell to identify potential terrorists. The applications outline networks of video, motion, chemical, and biometric sensors at airports that would feed into a local computer grid, yielding results in near real time. As described by Alex, the key technology IBM is seeking to patent is a software "inference engine" that uses heuristics and rules developed by the three co-inventors to crunch the data and sort out high-risk people.