Data analysis with safeguards

By David H. Schanzer

DURHAM

The revelation last week that CIA counterterrorism analysts are reviewing "tens of thousands" of confidential international banking records has highlighted once again the tension between security and privacy in the modern age.

Our fight against terrorism requires use of this modern technology. But if the government wants to maintain public support for these efforts, it needs to be less secretive and offer more privacy protection.

The public debate over the bank records program is both familiar and mundane. The government argues that the program is technically legal and vitally necessary. Civil libertarians decry privacy violations and claim the program is open to abuse.

POINT OF VIEW

Since this revelation about the banking program is probably not the last of its kind, it is time to end the accusatory hyperventilation and identify some principles to guide our future consideration of such programs.

The starting point for this discussion must be that we want the government to use high-tech data analysis tools to combat terrorism. When compared to other counterterrorism strategies — ranging from military conflicts that kill thousands and cost billions to baggage searches at airports, football stadiums and who knows where else — whizzing computer programs that don't inconvenience us and cost less than a single armored Humvee suddenly seem more attractive. Picture a 9/11 Commission-style hearing after the next attack and imagine our outrage when witnesses testify that we had, but failed to use, technological tools that would have uncovered the plot. Bottom line: The government should and will use this technology.

It is part of the American DNA, however, to be skeptical of government power. Heightened concern is to be expected when technology is used to sort through personal information of American citizens.

• • •

Consequently, the legalisms that the government puts forth to justify its programs are of little use. Like Justice Stewart's view of pornography, Americans know an invasion of privacy when they see it and it is entirely beside the point that the government is only reviewing information that has been disclosed to third parties like banks or telephone companies. People don't like the government having access to information about who they are talking to, what they are buying, or where they are going, even when "the government" is an anonymous computer sifting through millions of records in a matter of minutes.

Since feelings about protecting personal information are not going to change, there are a few basic principles that the government ought to follow if it wants to maintain public support for use of data analysis tools in the counterterrorism fight.

First, be transparent. The surest way to raise suspicion is to have a secret personal .data analysis tool revealed for the first time by the media. There must be a way for the executive branch to tell the people, and the people's representatives in Congress, about the tools we are using to track down terrorists without disclosing details that would enable al-Qaeda to evade detection. Congressional authorization of these activities would go a long way toward easing public concerns..

Second, build in safeguards. The public is rarely reassured by claims that a program is "narrowly targeted" at the terrorists and subject to multiple layers of "internal review." Data analysis programs should be subject to external and independent scrutiny. Although judicial review for every computer search is impractical, the government should be required to obtain a warrant before accessing broad classes of personal information, such as the international financial database at issue in the CIA program.

There also ought to be audit trails documenting who accessed what information so, if there ever are abuses, we can identify the guilty parties and hold them accountable. Congress and agency inspector general offices also should conduct rigorous oversight.

Finally, provide anonymity when possible. The claim of a privacy invasion is far less weighty when the government is sifting through data that has been stripped of personal identifiers. Only after the government identifies a suspicious transaction or pattern should the personal information be revealed.

A frank, honest discussion about how data analysis technology is to be used against terrorists or, for that matter, other criminal enterprises, is overdue. The government should welcome, not resist, such a discussion. As long as some basic protections are put in place, it's likely the public will strongly support these data analysis ~~tools as part of~~ our counterterrorism efforts.

David H. Schanzer is director of the Triangle Center on Terrorism and Homeland Security at Duke University and UNC-Chapel Hill.