



How to Conduct Surveillance of Terror Suspects

by **Daniel Gallington** (more by this author)

Posted 09/06/2010 ET

The recent round-up of a U.S. based Somali terrorist group—comprised of some U.S. citizens—reminded me of a conversation I had with my mother a few years ago.

My mom, who lived to be almost 90, and I were watching a TV news report on electronic privacy. She knew that I had spent a lot of my professional career developing the laws and policies that regulate our intelligence agencies collection of information “on or about U.S. persons.”

She said, “Daniel, I know that it’s your business, and not mine, but I don’t think that the government should be listening to anyone’s private conversations.”

Responding, I said, “OK, Mom—but what about spies, terrorists and criminals?”

She thought for a second and said, “Well, those kind of people ... of course.”

It occurred to me that this exchange was probably typical of most peoples’ thinking about the correct balance between privacy and protecting our society against those

who want to do us harm.

I could have asked her couple more questions to narrow it even more, i.e., “how about spies, terrorists and criminals and the people they are talking to and the people who are talking to them?”

She would probably have said, “OK, but how would you know if they really are criminals, spies or terrorists? And, some of the people they are talking to and who are talking to them might be talking about the weather, family matters or just to order a pizza.” Then, I would have said, “but how would you know that?” And she would have said, “you’d probably have to listen a while to find out, I guess.”

And there, in a nutshell, you have the essence of the implementing policies of NSA’s controversial “terrorist surveillance program,” certainly the gist of the policies that implement the Foreign Intelligence Surveillance Act (FISA) and even the more mundane criminal wiretap programs described by statute in both federal and state law—all simplified by my mom.

And, despite the attempts by the *New York Times* and others to describe it as the government violating everybody’s privacy, most people know better. Not only that, like my mom, they hope that we’re targeting the bad guys and the people talking to them about bad things—and not when they’re ordering pizza.

Specifically, the general public should take three basic points of learning to the stories they read about government surveillance programs: When I was “in the business” we called them the “three A’s”—articulation, approval and audit.

We need to know how the program describes, or articulates, the target of the surveillance, i.e., this is the “terrorist, spy, and/or criminal” part, and requires an extremely detailed description of (1) who the targets are, and why (2) what kinds of communications from and to them are of interest, and (3) by what means. The communications that are not of interest—e.g., ordering pizza—are “minimized”, a technical word for sorted out. The articulation is generally contained in the request for approval of the surveillance.

We need to know who approves the surveillance, and at what level of authority. Was it approved by (1) a court and/or (2) a senior official with the specific authority to approve it and what legal regime governs the approval for the surveillance? This category of issues is where spats between Congress and the President generally arise—the Congress saying that the surveillances requires a statute (e.g., FISA) and the President saying that the surveillances are part of his “commander-in-chief” powers in the Constitution. These disputes are usually more “proprietary” than they are substantive—more often than not, they are mostly political “turf” disputes.

Who audits or “oversights” the surveillance and how intensive is the regime that defines the audit requirements? This is “everybody’s business,” meaning that both the executive branch and the Congress must have very aggressive audit programs, because these independent examinations often result in more precise targeting, faster confirmation (or elimination) of threats and more effective use of limited surveillance resources, both human and technical.

The “three A’s” are of particular importance when dealing with surveillances of “U.S. Persons”, a category much larger than U.S. citizens, and includes foreigners who are here legally and foreign corporations comprised “substantially” of “U.S. Persons.”

In fact, many would argue that the whole concept of “U.S. Persons” is anachronistic in this day of “foreign-affinity terrorism”—these are the U.S. citizens who become active in foreign based terrorist organizations, or adopt its ideology, with the intention of carrying out terrorist acts in or against the U.S.

At the minimum, it seems very appropriate for both the President and the Congress, regardless of the party politics involved, to review the entire issue set associated with the idea of “U.S. Persons” and determine if changes in law, regulations and internal procedures are needed to address these new and very dangerous threats to our homeland.

I don’t think it would make much difference to my mom—or yours—whether the “spies, terrorists or criminals” we were watching were technically “U.S. Persons” or

not—as we have learned they can be just as deadly.

Daniel Gallington is a Senior Fellow at the Potomac Institute for Policy Studies in Arlington, Va.

[Advertise](#) | [Privacy Policy](#) | [Terms and Conditions](#)
Copyright © 2010 HUMAN EVENTS. All Rights Reserved.