Counterterrorism activities must harness technology to protect liberty

Matt A. Mayer

November 30, 2015 5:30 am | *AEI.org*

With the latest terrorist attack in Paris, how America improves its intelligence capabilities to detect and stop terrorist attacks is a top issue. Intertwined with that discussion is the reality that Americans face continued erosion of their privacy via “big data.”

We accept some of this erosion in exchange for the freedom to harness technology to make our lives easier to navigate and to connect with friends, family, and colleagues. We know that every transaction we make using our smart phones or computers is being tracked, analyzed, and embedded with cookies by private entities for future use.

When it comes to government programs, however, our acceptance is and should be lower. Equally important, our expectations of how government approaches the thorny problem of keeping us safe while respecting the Constitution should be very high. Too often we see technology as something that can be used against us. In this context, technology can be both a sword and a shield.

Yes, technology is being used both internationally and domestically to watch our enemies, detect terrorist threats, undermine rogue regimes, and analyze a stunning amount of data. At the same time, government should find ways to use technology to remove as many Americans as possible from broad-based counterterrorism programs. The continued debate over the collection of meta-data from telephone companies (http://video.foxnews.com/v/4404624763001/chris-christie-rand-paul-spar-over-nsa/?#sp=show-clips) would wither if we knew that the vast majority of Americans weren’t subject to it. Our suspicions would lesson if we knew that most of us had been deemed cleared.

Because virtually every monitoring program must use IP addresses and telephone numbers, government programs should be able to pre-emptively remove cleared digits so that data is not collected from those entities or is withheld by private entities. We shouldn't have to settle for an environment where we don't worry because we are innocent. Our Constitution deserves a basis greater than mere presence for monitoring us or collecting our data, no matter how innocuous or how many safeguards get built to prevent illegal searches.

Fundamentally, for Americans to be subject to counterterrorism programs, there should be a precursor nexus to suspected terrorist activity that adds them to monitoring and data collection programs. Here are a few activities that most Americans never engage in:

- Travel to and from certain high-risk countries
- Visiting jihadi websites
- Following or friending terrorist associated groups or individuals on social media
- Sending and receiving telephone calls, emails, or texts from certain countries
- Using certain words or phrases in Internet searches
- Buying certain components or compounds without demonstrated need (e.g., a farmer in Iowa routinely buys fertilizer)

In each case, inclusion in government programs is based upon specific acts, not mere presence. The benefits of this approach are enormous.

First, there is little proof that broad-based government programs have increased our domestic security. More often, we've simply gotten lucky that the bomb did not go off (e.g., the Detroit shoe and Times Square bombers). When we have stopped a terrorist attack, it is more likely that specific actions by terrorists resulted in their detection (e.g., sending and receiving direct messages on Twitter with known terrorists).

Without proof of clear benefits of broad-based monitoring programs, America should always default to freedom over marginal security improvements. Because most Americans have no nexus or even six degrees of separation to terrorist activities, they should be free from government monitoring or data collection.

Next, the fundamental problem of big data is the ratchet effect of the sand pile. As increasing technology usage generates more data, government programs require more refined analytics to sort through the data. Imagine your job is to find a pearl in a car-sized sand pile. You start by using a hand shifter to sort through the sand. A day later, however, a dump truck adds a ton more sand to the pile. You'll need more than a hand shifter to find the pearl. Unless you find a way to reduce the amount of sand being added each day, your odds of finding the pearl get reduced to pure luck.

Our intelligence community must be able to find the various pearls and connect them before an attack. We shouldn't spend billions on government programs that undermine our civil liberties to get ourselves to the same position we were in beforehand. If we are going to do something, it must get us past lucky.

Finally, it shows Americans that our government understands we are entering a brave new world in which it will be increasingly easy for government to leverage technology to do any number of things. Demonstrating restraint now and embedding the concept of restraint into the culture of our government agencies will increase the odds that our future won't be one painted by the hardcore civil libertarians.

Moreover, when the next leak occurs of a heretofore unknown counterterrorism program, it will lessen the outrage and suspicion if the government can state that it limited the scope of the program to a small group of Americans based on a nexus to terrorist activity.

It is time technology gets used to lessen the government's interest in our lives and in the data that gets generated from us doing everyday activities. The vast majority of Americans don't and will never have a nexus to terrorist activity. They shouldn't, therefore, have their lives subjected to any monitoring or data collection, no matter how insignificant government actors claim it is.

Our Constitution and way of life require that our government meets a much higher standard than we willingly tolerate in other spheres of our lives. A year from now, a new president-elect will begin the transition process. A priority of that administration should be to restore the confidence Americans have in their government to protect their privacy.

By leveraging technology, we can strike a better balance between security and liberty.

This article was found online at:
http://www.aei.org/publication/counterterrorism-activities-must-harness-technology-to-protect-liberty/