ODNI Review Group Comments
Richard B.

Dear Members of the Review Group on Intelligence and Communications Technologies,

I am slow. If I had run the Boston Marathon again this year, I would have just passed the explosions when they went off. I watched the events of the following days closely, as so many of my close friends were affected by the bombing. I was heartbroken when I learned that information available on the bombers went ignored by federal law enforcement. Such tragedies must be prevented whenever possible.

The NSA's desire to collect ever more data is a prime example of the Haystack Fallacy: the absurd notion that you will find more needles by piling on more hay. More data would not have stopped the Marathon bombing. If anything, it appears too much data prevented effective action. The key information was hidden in plain sight. How many other opportunities to save lives have been lost because the vital details were buried in endless chaff? We want and need our intelligence community to be more effective. But effectiveness will not come from piling on more hay.

As an MIT alumnus, former hospital employee, software developer, and current privacy officer, I do have a little understanding of the balance between privacy and security concerns. Privacy rights and national security should not be opposed; indeed, I believe they go hand-in-hand. Collecting less data and doing more analysis can enhance both. Through the recent leaks, we have learned that the bulk of the intelligence budget goes toward collection activities, with a minor part toward analysis; that ratio ought to be reversed. To truly make intelligence technologies effective, however, a change of priorities is needed.

The best way to protect our national security and advance our foreign policy is not to create the terrorists who target us in the first place. A madman with a bomb does not become a terrorist unless he feels personally injured by a country's policies and practices, so a necessary first step is to shift focus from tracking the actions of terrorists to evaluating the actions of our own government.

Here are some key questions to ask: 1) How does the government create terrorists through our policies and practices? 2) Which policies and practices have the greatest risk of creating terrorists? 3) How can we estimate how many terrorists will be created through a given policy or practice? 4) How can we change a given policy or practice to reduce the threat it will create new terrorists? 5) How can we change a given policy or practice to reduce the threat it will motivate new attacks?

Currently, the intelligence community is ill-equipped to answer these questions, but such answers are vital to protecting our national security and advancing our foreign policy effectively. The intelligence community should develop quantitative measurements of the terrorist threat produced by each foreign policy or practice that is enacted. Then such information needs to be conveyed persuasively to policy makers for their consideration and adaption. This requires a vastly different skill set and mission focus than the

intelligence community currently has available. Still, if we prevent people from being driven to terrorism, we will need far fewer resources applied toward fighting it. Ensuring national security is, at its heart, a social problem, not a technological one.

For those few cases where privacy-breaching surveillance remains necessary, here are a few more social protections I would suggest for minimizing harm: 1) Avoid "Too Many Secrets": Policies should never be secret. Openness is essential to democracy and freedom. Moreover, secrets are illusions; they are always lost given sufficient time. The only way to avoid a breach is to avoid having a secret to breach in the first place. Openness is also the best way to gain quick feedback and clarity on how effective a policy is. 2) "The Golden Rule:" Treat others as you would have them treat you. Don't make enemies. This is best way to ensure that foreign entities will treat us well. Privacy is a universal human right, not just a right of US citizens; protecting the privacy and security of all will help ensure our own national security. 3) "Always Three to See:" No analyst should ever have any access to intelligence data alone. Requiring three analysts to concur on accessing any item of data would go a long way to preventing privacy breaches as well as security leaks. Three heads are also much better than one at spotting a needle in a haystack. (This is one step further than the proven effectiveness of pair programming techniques used in software engineering, but the extreme seriousness of national security requires an even higher level of agreement.) The "Always Three to See" rule should be applied not only to reviewing and analyzing data, but also to every activity of the intelligence community: data collection, data storage, cryptography, technology development, policy formation, etc. Another more general way of phrasing this is to "avoid a single point of failure."

I could go on and add countless other suggestions, but I think this might be a sufficiently good start. If you consider these 5 questions and 3 guidelines in all your work, I am sure you will be well on your way to optimally protecting our national security and advancing our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure. I realize a journey in this direction toward a more effective and open intelligence community will likely be painfully difficult and slow. Persist, and you will succeed, as any marathoner can you.