

## BIOMETRICS TALK

I want to talk about your topic – biometrics – from the perspective of someone who focuses on trying to prevent bioviolence. I also want to talk about this topic as yet another example of what I think is a most important question of our age: how can we ride the crest of an amazing wave of technology, taking advantage of its wondrous benefits while minimizing the risk of a catastrophe?

What I do not want to talk about today is the use of biometrics to combat terrorism or crime generally, to monitor borders, immigration, customs control. There are substantial differences, after all, between focusing on ethics/privacy implications of new science and on security implications positive/negative of new science. Obviously, systems that are designed to reduce threats of terrorism and crime generally will have implications for reducing threats of bioterrorism, but the use of biometrics in this context has already been well-discussed, and there's not much that I, as someone uniquely focusing on bioterrorism, can add.

First, just a few comments about what are the characteristics of bioterrorism that distinguish it from other types of threats and that call for distinguishing tactics.

1. More than any other type of threat, the mechanism is essentially invisible. Security measures cannot, realistically, focus on detecting the agent; security measures must focus on perpetrators.
2. These perpetrators might be “known” terrorists that might be identifiable with border security measures, including biometrics; far more likely, however, bio-perpetrators will be individuals who are completely and entirely unknown, meaning that biometric detection will not necessarily enable the security measures that we expect in other contexts.
3. There are a whole group of “perpetrators” – and I use that term somewhat facetiously to make a point – who are altogether unaffiliated with terror networks: these are the unknowing carriers of contagious disease. These people need to be stopped, not because they are malevolent, but because they are contagious.
4. From the perspective of malevolent perpetrators, bio-laboratories are critical. Although pathogens are, of course, ubiquitous, if a perpetrator really wants to commit a catastrophic attack, he has to either get laboratory-refined pathogens or get into a laboratory to weaponize them himself.
5. As I've already implied, bioterrorism is a uniquely global threat. Of course, in our shrinking world, just about any weapon can be used just about anywhere, but pathogens can come from anywhere, be smuggling just about everywhere. More important, the effects of a catastrophic bio-attack will have trans-national implications. Every other weapon, no matter how horrific, is confineable in space and time. It's awful for the victims, but if you aren't there, it's effect on you is grief and rage but not personal peril. But a contagious attack puts everyone at risk everywhere.

So, with these considerations in mind, let me pose some questions about biometrics and bioterrorism.

1. A problem re bioviolence has to do with packaging and labeling pathogens for shipment. WHO has had substantial success in promulgating guidelines for how pathogens are to be shipped and spread that information around the world. WHO's success has generated two problems, however. First, malevolent persons can have ready access to this information and can fraudulently cover their smuggling by preparing legitimate-looking packages. Second, proper packages can be easily identified by any potential thief. There is a need, therefore, to mark pathogens with coded symbols. They will have to be marked, of course, at the point of shipment, and those markings will have to be identifiable at key junctions all the way through to their destination.

There are two questions for biometrics. First, can biometric technology be useful in meeting the challenge of marking pathogen shipments? Second, because of the increasing sophistication required for every step along the shipment route, all workers along the way will need to be trustworthy. Workers will have to be registered with biometric information stored in secure databases (Safe Ports Act). So, there is a relationship between packaging-labeling-shipping security and transportation security.

2. The second question is related: can biometrics be interoperable with disease sensors, biosurveillance, and forensic technologies. For example, can the finger swipe that a foreigner goes through at border controls be enhanced so that it will pick up indications that the person is carrying a contagious disease.
3. The use of biometrics for laboratory security has been well-addressed. Biometrics can offer useful ways to ensure that only select individuals get access to particularly dangerous pathogens. The question is whether it would be effective to implement a legal obligation on labs to install biometric screening. If so, can these biometric systems be proactive – i.e., the systems know when they've been attacked or dismantled.
4. Biometrics for building security
5. Biometrics for data collection and analysis
6. Can biometrics be misused by bio-offenders?
7. Can new science have benefits for development? If so, what are the mechanisms/implications of spreading that science to developing communities?