



ACLU Backgrounder on Body Scanners and “Virtual Strip Searches”

Following the attempted terrorist attack by Umar Farouk Abdulmutallab in December 2009, the Transportation Security Administration is integrating “whole body imaging” machines into routine airline security procedures. The ACLU opposes the widespread use of this technology.

- This technology involves a direct invasion of privacy. It produces strikingly graphic images of passengers’ bodies, essentially taking a naked picture of air passengers as they pass through security checkpoints. It is a virtual strip search that reveals not only our private body parts, but also intimate medical details like colostomy bags. Many people who wear adult diapers feel they will be humiliated. That degree of examination amounts to a significant assault on the essential dignity of passengers. Some people do not mind being viewed naked but many do and they have a right to have their integrity honored.
- The likely effectiveness of such a technology in preventing attacks does not justify the level of intrusion involved. It is far from clear that body scanners would have detected the “anatomically congruent” explosives Abdulmutallab hid in his underwear. Some experts have said explosives can be hidden by being molded against the human body, or in folds of skin, and British newspapers are reporting that government testing in the UK found that the technology comes up short in detecting plastic, chemicals and liquids. At London’s Heathrow airport, a four-year test of the scanners resulted in a decision to discontinue their use.
- Body scanners should not be used as part of a routine screening procedure, but only when the facts and circumstances suggest that it is the most effective method for a particular individual. And such technology may be used in place of an intrusive search, such as a strip search – when there is reasonable suspicion sufficient to support such a search.
- Terrorists will easily evade body scanners in other ways. The terrorist threat is a dynamic threat – terrorists react and adapt to security measures, and that fact must be taken into account in selecting those measures. If scanners are perceived to be effective, terrorists could conceal explosives in their body cavities. Al Qaeda has already used this technique; in September a suicide bomber stowed a full pound of high explosives and a detonator inside his rectum, and attempted to assassinate a Saudi prince by blowing himself up. And terrorists could shift their efforts to just hiding explosives in their carryon baggage; the TSA’s level of success in catching contraband has always been mixed. Study after study by DHS’ internal investigators, as well as independent investigators, have found that TSA still cannot identify a large majority of explosives and weapons that the testers have sought to bring through security. And reliably catching every possible means of hiding a few ounces of explosives is probably impossible given the millions of people who fly each day.
- The practical obstacles to effective deployment of body scanners are also considerable. Domestically in the United States alone, 43,000 TSA officers staff numerous security gates at over 450 airports and over 2 million passengers a day. In order not to be an ineffective “Maginot line,” these \$200,000 machines will need to be put in place at all gates in all airports; otherwise a terrorist could just use an airport gate that does not have them. Scanner operators face the constant problem of boredom and inattention when day after day, year after year, no terrorists come through their gate. In addition to the expense of buying, installing and maintaining these machines, additional personnel will have to be hired to run them (unless they are shifted from other security functions, which will degrade those functions).
- TSA is also touting privacy safeguards including blurring of faces, the non-retention of images, and the viewing of images only by screeners in a separate room. Scanners with such protections are certainly far better than those without. However, we are skeptical of the privacy safeguards that the TSA is touting:

- Obscuring faces is just a software fix that can be undone as easily as it is applied. And obscuring faces does not hide the fact that rest of the body will be vividly displayed.
 - A policy of not retaining images is a protection that would certainly be a vital step for such a potentially invasive system, but given the irresistible pull that images created by this system will create on some employees, how much assurance can we really have that images are not going to end up on the Internet? Unfortunately, the government's record of safeguarding private information is not great.
 - Intrusive technologies are often introduced very gingerly with all manner of safeguards and protections, but once the technology is accepted the protections are stripped away. That is especially likely with regards to protections that might reduce security, such as relying on automated visual pattern recognition instead of human beings to look for contraband.
- The TSA should invest in developing other detection systems that are less invasive, less costly and less damaging to privacy. For example, "trace portal detection" particle detectors hold the promise of detecting explosives while posing little challenge to flyers' privacy.
 - Security is never absolute and never will be. It is not wise security policy to spend heavily to protect against one particular type of plot, when the number of plots that can be launched – not only against airlines, but also against other targets – is infinite. Limited security dollars should be invested where they will do the most good and have the best chance of thwarting attacks. That means investing them in developing competent intelligence and law enforcement agencies that will stop terrorists before they show up at the airport.
 - The government must indeed work zealously to make us as safe as possible and to take every reasonable step to make sure security breaches do not happen. But we need to act wisely. That means not trading away our privacy for ineffective policies.

American Civil Liberties Union of New Jersey

P.O. Box 32159, Newark, NJ 07102

973-642-2086

www.aclu-nj.org • info@aclu-nj.org

November 2010