Defending democracy

Government surveillance technology programmes must aim to protect privacy and civil rights from the start, says **Daniel Sarewitz**.

Notwithstanding the incompetence of last month's New York City would-be bomber, the terrorist threat is real. One way governments try to meet this threat is with improved security technologies that keep track of terrorists' movements and communications. But these same devices will also be monitoring innocent people, and so can threaten privacy and civil rights. Will less freedom be an unavoidable side effect of powerful new surveillance technologies?

Not necessarily — but the time to start thinking about the impact of security technologies on democratic rights is during research and development (R&D), not after the devices have been introduced into society. Ji Sun Lee, a lawyer at the US Department of Homeland Security (DHS) in Washington DC, is trying to do just this.

Up to four times a year, Lee convenes a 15-person 'community acceptance of technology panel' to gather feedback on the social implications of one of the DHS's 140 technology projects. Panellists include experts in the social aspects of security and surveillance, as well as representatives of interest groups who might be particularly affected.

Not exactly reassuring

Some projects are pretty spooky — perhaps none more so than Future Attributes Screening Technology (FAST, see *Nature* **465,** 412–415; 2010). Using physiological indicators such as heart rate and breathing, these devices would screen individuals at stadiums, airports and other possible terrorism sites for what the DHS inelegantly calls "malintent". Lee rejects my suggestion that FAST is leading the DHS into the territory of *Minority Report*, a movie in which authorities monitor citizens to predict crimes before they happen. But when I ask her about political and ethical concerns raised by her FAST panel, the DHS public-affairs officer monitoring our interview interrupts, saying: "We're not going into that level of detail." Such interdictions do not relieve one's paranoia.

Hardly less worrisome are 'mobile biometrics' devices. These portable technologies will gather information, such as fingerprints, iris scans and facial images, and feed them into national databases to make rapid identifications and threat assessments. "The potential for abuse is massive," says Nihad Awad, executive director of the Council on American–Islamic Relations in Washington DC, and a participant in Lee's 2008 mobile-biometrics panel. "How are the data stored, who gets access to them, what sources of oversight exist?"

Similar questions emerged when Lee convened a panel on detecting terrorists at the US–Canada border. Panellists considered the implications of video surveillance along remote, unfenced parts of the border. They also discussed a DHS proposal to embed radio-frequency identification chips in the registration cards of vehicles and boats owned by Americans living near the border. The chip programme would allow more efficient monitoring of border-area security threats because US authorities could focus surveillance on vehicles without chips — but this would also turn every vehicle owned by a Canadian into a target of suspicion.

Not surprisingly, Canadian panellists didn't want "the US government to be spying on Canadians doing whatever it was they wanted to do in the backwoods" and border towns, recalls panellist David Mutimer, a political scientist at York University in Toronto, Ontario. To make matters worse, the DHS gave no assurances about how the data would be used and privacy protected.

"The time to start thinking about the impact of security technologies on democratic rights is during R&D."

Have the panels had any effect? Lee says that the panels provide recommendations to programme managers, but they don't have authority to terminate a project or dictate how technologies are developed. Awad and Mutimer feel that the process could be valuable, but neither has heard anything from the DHS since their panels, and they have no idea if their deliberations made a difference. Lee's boss, Sharla Rausch, head of the Human Factors/Behavioral Sciences Division, does say that one DHS project was substantially changed as a result of panel recommendations, but she will not provide specifics.

In any case, one-off panels are not enough. Ongoing and interactive partnerships between panellists and technical teams are necessary. Awad, an engineer by training, is sympathetic to the idea that more-inclusive discussions could reduce some negative aspects of security technologies. But he emphasizes that panellists need to see the effects of their involvement so that they can develop trust in the process. For example, the American–Islamic council was strongly opposed to body scanners at airports because they violated Islamic rules on modesty. "If we had been involved in discussing the technologies from the beginning," Awad says, "we would have suggested that the software be designed to blur the images, and this would have avoided much controversy".

Privacy by design

The idea of R&D programmes that simultaneously consider technical prospects and social implications is hardly novel. In 1947, Detlev Bronk, head of the National Research Council, made this point in testimony to Congress: "Social scientists should work hand in hand with natural scientists, so that problems may be solved as they arise, and so that many of them may not arise in the first instance." In reality, the problem is less one of social-science research than of opening up the innovation process to a variety of informed perspectives. But the important point is that unless R&D programmes include consideration of social impacts at an early stage, scientists and engineers will miss opportunities to develop more socially desirable technologies.

More than 60 years later, Lee's programme is a modest but hopeful step in this direction. Despite the DHS's self-defeating fear of transparency, Lee is working to figure out how to identify, discuss and address complex social dangers before they get locked into the new technologies.

But to really make a difference, her programme — among the smallest in the DHS's billion-dollar science and technology directorate — would need to be ramped up to become a full partner in all of the agency's technology development. It would need to consider many more technologies, and do so in an open, integrated and persistent manner, rather than through single panels. Such a mainstreaming process might go a long way towards relieving the irony of technologies that protect citizens' lives even as they threaten their rights. ■

Daniel Sarewitz, co-director of the Consortium for Science, Policy and Outcomes at Arizona State University, is based in Washington DC.
e-mail dsarewitz@gmail.com.

See go.nature.com/ILx8PC for more columns.