nature nanotechnology

Vol.2 No.1 January 2007

www.nature.com/naturenanotechnology

Beware of big brother

Security and surveillance are emerging as major and sometimes controversial applications of nanotechnology, especially in the United States. Although some of these applications are to be welcomed, others should be handled with care.

As the Tuesday night poster session was getting started at the Materials Research Society (MRS) meeting in Boston at the end of November 2006, a rather different event was in full flow at the Museum of Science elsewhere in the city. A panel of 12 people with very different backgrounds — including three leading nanotechnology researchers— was taking part in a seminar called 'Nanotechnology: The Power of Small'. This event was interesting for many reasons, including the way in which it reinforced the impression that nanotechnology is much more closely associated with security and defence in the United States than it is anywhere else in the world. The number of symposia at the MRS meeting sponsored by the US Army Research Office and other similar bodies adds to this perception, although the US military has a long track record of supporting basic research, much of which gets presented at meetings and published in the literature.

The format of the seminar at the museum also differed from the standard approach in which a panel of experts all say 'a few words' and then take 'some questions' from the audience. For a start, in addition to the three researchers, the panellists included a local politician, a senior homeland security official, a law professor, the co-founder of Families of September 11 and a director from the American Civil Liberties Union, among others. Moreover, a moderator presented the panel with a series of scenarios that explored the different ways in which the use of nanotechnology for security and surveillance applications might influence our lives, starting with a debate about implanting nano-enabled tracking devices into the arms of elderly people living on their own so that their families could keep track of them. Other scenarios discussed during the seminar included a hypothetical smart credit card that collects enormous amounts of information about the lives and spending habits of teenagers, and the possible introduction of airport-style security into everyday train travel. Finally, the whole event was filmed and will be broadcast on American television as a 'Fred Friendly Seminar'.

The underlying assumption — which no one challenged — was that nanotechnology would make it easy (and cheap) to collect, store and process vast amounts of personal data that could be used by governments and companies for surveillance and marketing purposes. However, there are still major technical challenges related to the development of techniques and software that can analyse and understand all these data. This brings into sharp focus all manner of well-known ethical questions about how much data should be collected and who should have access to these data.

It is in no one's interest for nano to be seen primarily as a 'big brother' technology.

Although consumers can either accept or resist these moves in the marketing arena, depending on personal preference and circumstance, there is no such choice when it comes to surveillance. In the past, police forces and security agencies have mostly used technology (for example, CCTV cameras and DNA evidence) to investigate crimes, including acts of terrorism. However, advances in technological performance combined with the increased threat of terrorism have led to a new emphasis on the use of technology to detect crimes and acts of terrorism in advance.

There is no doubt that developing new nanosensors to detect nuclear, chemical and biological weapons is to be welcomed, and real progress is being made on the detection of everything from gamma-rays and neutrons to anthrax and other pathogens. However, when nano and other technologies are used to collect and store more and more information about individuals in the name of security, the benefits are not so obvious because design flaws (or determination on the part of a terrorist) will mean that no system is ever 100% reliable. If complete reliability were possible there might be a case for trading-in some civil liberties but, in general, they should not be given up lightly. It is also pertinent to ask if the money required to build an all-seeing surveillance system could be better spent on other approaches.

It is important that the nanotechnology community takes an interest in debates like these because it is in no one's interest for nano to be seen primarily as a 'big brother' technology, especially when a large number of medical, environmental and other applications are being developed. Indeed, adverse press coverage of a nanosecurity workshop in Germany in 2005 caught researchers unawares and forced the Max Planck Society to look into the defence and security aspects of nanotechnology research. In future it will pay to be prepared.