

Submission  
No 26

## INQUIRY INTO NANOTECHNOLOGY IN NEW SOUTH WALES

**Organisation:** University of Western Sydney  
**Name:** Mr David Vaile  
**Date received:** 10/06/2008

---

Filed by Mr David Vaile  
10.6.08.  
D.V.

## **Nanotechnology and consumer privacy: some examples**

Submission by David Vaile, Cyberspace Law and Policy Centre, UNSW

Tuesday, 10 June 2008

### **Avenues through which Nanotech can erode consumer privacy.**

The most common criticisms held by consumers are concerns that 'the use of this technology is premature, and should require ironclad proof of safety'<sup>1</sup>. The loss of personal privacy is one of the public's fears about nanotechnology, as new sensing and surveillance technologies are developed on a regular basis<sup>2</sup>. The potential applications of nano-tech are not fully understood or imagined.

Some practical challenges to consumer privacy already exist in relation to potential applications of nanotechnology.

#### **Nano-Diagnosis**

- Concerns already exist about genetic and other discrimination. This is particularly important in the US where the health sector is completely privatised. If Nano-enabled diagnostics devices are developed people may feel as though they need to choose between privacy and medical care.

○

The role of the executive: homeland security.

- The U. S. National Nanotechnology Institute (NNI) recently received a \$5 billion grant from congress to hasten the discovery, development and deployment of nanotechnology in order to promote (amongst other things) national security.
- The US National plan aims to create a system that "at its heart would be a sensor network that is intelligent, self-monitoring, and self healing to allow continuous operation for situation monitoring and information transfer"<sup>3</sup>
- With the advent of nano-tech not only will it be possible to process vast amounts of personal data, it will be possible to do so in real time, giving law enforcement agencies unprecedented capabilities to engage proactively<sup>4</sup>.
- The NNI outlines its goal as "dynamic situation control", an ambitious plan to collect vast amounts of data from people, objects, and sensors,

<sup>1</sup> From submission by Leslie McCawley to the committee at:

[http://www.parliament.nsw.gov.au/prod/parliament/committee.nsf/0/0fc3ad5c2683ae9dca257426007f3ddd/\\$FILE/Submission%205.pdf](http://www.parliament.nsw.gov.au/prod/parliament/committee.nsf/0/0fc3ad5c2683ae9dca257426007f3ddd/$FILE/Submission%205.pdf)

<sup>2</sup> From healy article, he refers to surveys in footnote 1 and 2.

<sup>3</sup> U.S., Nanoscale Science, Engineering and Technology Subcommittee, Committee on Technology, National Science and Technology Council, The National Nanotechnology Initiative Strategic Plan (2004) at 24.

<sup>4</sup> Campbell page 1.

analyse this data and then infer actions or intent so as to control the outcome of a given situation.<sup>5</sup>

The above definition of dynamic situation control illustrates many of the privacy concerns surrounding nano-tech. The goal is to grant greater population surveillance and management control to the possessor of the technology: the US government.

In the US the governments desire to collect a wide array of information reflects an claim that individual processing is ineffective when using raw characteristics such as race alone<sup>6</sup>. (Less frequently asked is whether their plan for 'control' is possible on any scale, but the quest seems to drive ever more intrusive plans.)

It is more likely that the future of government surveillance will move towards data processing, attempting to narrow down members of lots of different groups, and gaining more information about individuals than is currently available: It is in these areas (data processing and acquirement) that Nano-tech is likely to be applied by NNI.

Whether these two issues (Nano-diagnosis, and Nano-surveillance) will be relevant privacy concerns in New South Wales is unclear, though it is clear from the US experience that whatever its application Nano-tech has considerable implications upon privacy.

### **Conclusion**

Nanotech is a general purpose technology, which means it's difficult to determine with certainty how it will be implemented and developed in the future on a commercial scale. This means regulation over the Nanotech industry is an inherently difficult process, which will constantly need to be updated as new markets are evolving – the technology has the capacity to move anywhere, and as a consequence it is advisable for parliament to demonstrate caution when mapping out the industries future within NSW.

The precautionary principle should apply to Nanotech, as it does too many emerging areas of scientific industry where potential harm is significant and knowledge incomplete. Whilst the potential harms and advantages are unknown, the industry should step very carefully and cautiously in any potential commercial endeavours – granting considerable weight to the (frequently justified) fears of the public, which are often reasonably based on the uncertainty of experts.

---

<sup>5</sup> U.S., Nanoscale Science, Engineering and Technology Subcommittee, Committee on Technology, National Science and Technology Council, The National Nanotechnology Initiative Strategic Plan (2004)

<sup>6</sup> Capmbell, page 7.