

# Nanotechnology and the United States National Plan for Research and Development In Support of Critical Infrastructure Protection

Lisa Madelon Campbell<sup>†</sup>

In an effort to predict and avert threats to national security, governments in general, and that of the United States in particular, have devoted considerable resources to developing technological systems that gather information about individuals. In the past five years, the U.S. government has collected information about the movement of individuals across and within its national borders from various sources, including border security stations, law enforcement officials, and immigration authorities. Until recently, it seemed impossible for the U.S. government to draw useful analyses from all of the data it is collecting. The sheer volume and complexity of the information made it appear unworkable to perform an analysis in time to act pre-emptively. Now, developments in computing technology suggest that not only will it soon be possible to collect and process vast amounts of data, it will be possible to do so in real time, giving law enforcement officials unprecedented capacities to engage proactively.

This paper will examine the ways in which nanotechnology will likely revolutionize the computing industry, and the effect of these developments on the U.S. government's collection, processing, and dissemination of information about individuals for national security purposes. In an earlier article,<sup>1</sup> I examined the rising use of biometric, or physiological, data by governments in order to track individuals. One of the problems discussed in that paper was that while governments might collect vast amounts of information about individuals, they lacked the capacity to usefully process and analyze that information. Developments in nanotechnology are likely to change that.

This paper also considers the importance of engaging the public in the development of emergent nanotechnologies, due to privacy and health implications, and also because of the growing realization on the part of the scientific establishment that the success of any new technology depends in large part upon its acceptance by the community as a whole.

## The Science of Nanotechnology

In order to understand how nanotechnology will forever alter methods of computing, it is necessary to first examine the science. In essence, scientists have discovered that at the level of the ultra-small, there exist computing capacities that far outstrip the storage and processing capacities of the most powerful computers in operation today. As is discussed below, in an interesting intersection between biology and technology, nanotechnology employs organic cells to create computing devices that will be able to store and process vastly greater amounts of information than existing computers.

The ideas underlying nanotechnology were first described in ancient Greece by Democritus of Abdera (ca. 460-370 BCE), when he posited that all matter was composed of distinct, minuscule atoms, and the word "nano" stems from the Greek word for dwarf.<sup>2</sup> A nanometre is one-billionth of a metre, and nanotechnology involves the analysis and manipulation of matter at sizes approximately 1 to 100 nanometres.<sup>3</sup>

In the late 1950s, the Nobel prize-winning physicist Richard Feynman talked about rearranging atoms for information storage purposes.<sup>4</sup> Three decades later, the modern field of nanotechnology was born with the publication of K. Eric Drexler's *Engines of Creation: The Coming Era of Nanotechnology*.<sup>5</sup> He initially described the devices that would allow atoms to be bound together into a multitude of stable patterns as 'assemblers'. Drexler later formulated an intricate description of molecular manufacturing that would become possible through the use of these assemblers.<sup>6</sup> As he describes it:

Nature shows that molecules can serve as machines because living things work by means of such machinery. Enzymes are molecular machines that make, break, and rearrange the bonds holding other molecules together. Muscles are driven by molecular machines that haul fibres past one another. DNA serves as a data-storage system, transmitting digital instructions to molecular machines, the ribo-

---

<sup>†</sup>Counsel, Department of Justice Canada. The views and opinions expressed in this paper, prepared for the *Canadian Journal of Law and Technology*, are solely those of the author and do not necessarily represent the views and opinions of the Department of Justice.

somes, that manufacture protein molecules. And these protein molecules, in turn, make up most of the molecular machinery just described.<sup>7</sup>

Nanotechnology operates on a minute scale: atomic and molecular levels, or 1/100 nanometre, can be compared to 1/100,000 of the diameter of a human hair.<sup>8</sup> Proteins and Deoxyribonucleic-acid ("DNA") are usually from 5 to 200 nm, whilst blood cells are 5,000 to 10,000 nm in size. Nanotechnology is not simply science on a minute scale; it is the manufacturing of materials and processes that have chemical and biological aspects that differ from manufacturing as we know it.<sup>9</sup>

Completely distinct from traditional forms of manufacturing, nanotechnology looks instead to biology as a model, organizing atoms and molecules to create sophisticated constructs that can perform extremely complex operations.<sup>10</sup> Nanotechnology is already in use in a number of diverse applications, including the titanium dioxide used as a transparent ingredient in sunscreen that cannot be seen when applied to the skin, and faster, smaller-sized computer memories.<sup>11</sup>

## The Nanotechnology Industry

To date, more than 20 countries have developed nanotechnology programs, and the annual collective investment globally is estimated at \$4 billion.<sup>12</sup> United States government officials have compared the probable socio-economic impacts of nanotechnology to the Industrial Revolution. In 2004, the global financial impact of nanotechnology was estimated at between \$20–\$50 billion in revenues.<sup>13</sup> The Japanese government is the biggest spender on nanotechnology among Asian countries, and their funding in the fiscal year 2003 outstripped the United States at \$13 billion.<sup>14</sup> In its financing and regulation of emerging nanotechnologies, the European Union takes a somewhat different approach from the United States and Japan, placing greater emphasis on the potential returns to society.<sup>15</sup>

Over the last six years in the U.S., government spending for nanotechnology has nearly tripled, and the 2007 budget request for nanotechnology research and development is close to \$1.3 billion.<sup>16</sup> The U.S. government is by far the heaviest investor in nanotechnology in the United States.<sup>17</sup> As the U.S. director of the Office of Science and Technology Policy has observed, "investments in nanoscale science and technology research and development are essential to achieving the President's top three priorities: winning the war on terrorism, securing the homeland, and strengthening the economy".<sup>18</sup> Put another way, the federal government seeks to exploit the potential of nanotechnology for broad economic and national security purposes.<sup>19</sup>

## Molecular Computing Made Possible

Computing has evolved tremendously in the past three decades, and a concept called Moore's Law, or the doubling of transistor density every year and a half, developed as observers witnessed the increasing computing capabilities of devices currently in use. Put simply, "the computational power that \$1,000 buys has doubled every two years".<sup>20</sup> Both size and cost have been reduced over time; a transistor that cost \$1.00 in 1968 cost a mere ten-thousandth of a cent in 2002.<sup>21</sup>

However, the physical limits of the traditional semiconductor computer chip will soon be reached: it is impossible to fabricate smaller chips and maintain the same computing capacity. Because of this, molecular electronics, or computing on a cellular level, will become the next paradigm. Nanotechnology applications will increase the performance of electronic memory and embedded intelligence systems at a greatly reduced cost. As an example, a company based in Vancouver, Canada, is building a quantum computer with thumbnail-sized chips that will have more computing power than the aggregate of all computers built to date.<sup>22</sup>

Several computing firms are currently developing memory chips that are based on carbon nanotubes and that would vastly increase the storage capabilities of mobile devices.<sup>23</sup> To make carbon nanotubes, tiny sheets of graphite are rolled into extremely narrow cylinders that are mere nanometers in diameter. Their small size and efficient conductivity make them well-suited for use in electronic devices.<sup>24</sup> Abandoning the process of placing transistors onto silicon, these new technologies will rearrange molecules and atoms, carbon and other materials, enabling them to act as transistors, wires and processors that will be exponentially more powerful than computers we have today.<sup>25</sup>

In 2003, scientists in Israel announced that they had created a molecular computing machine that could be programmed and that was over 100,000 times faster than the fastest PC. Using a single DNA molecule as software, and enzymes as hardware, the chemical reactions that occur when these are mixed together allow them to perform computing operations.<sup>26</sup> While many applications are in development, some nanomaterials and technologies are currently in use. For example, the storage capacity in most computers can now be increased through the use of nano-thin layers of magnetic materials.<sup>27</sup>

This reduced size and increased computing capacity also has implications for the ways in which computers are used. The devices that are used to access the world-

wide web are becoming increasingly smaller and differentiated, such that they will soon be able to be incorporated, in a subtle and unobtrusive way, into the environment in which we live. Significantly, these computational devices can now sense information about the physical world in which they are situated, including visual images, sounds, and changes in temperature and electromagnetic resonance.<sup>28</sup> They have been described as “a digital nervous system grafted onto the material world”.<sup>29</sup>

What we can expect, then, are networks of miniaturized, wirelessly interconnected, sensing, processing, and actuating computing elements kneaded into the physical world. This animated control loop — of sensing data, processing it, then responding to it — can take place without direct human intervention or delay.<sup>30</sup>

The development of nanosensors, which would allow for accurate and instantaneous monitoring of events such as chemical warfare initiatives, is already underway.<sup>31</sup> Sensors will soon be built into a vast array of materials, such as gas sensors in motor vehicle engines and chemical detectors in water supplies.<sup>32</sup> Some predict that this will allow for the development of so-called “pervasive computing”, where the primary communications device would be a more sophisticated version of today’s hand-held computers. These more evolved devices would be telephones, and provide access to the worldwide web as well as to various networks and databases. The primary impediment to the development of this technology is the challenge of providing sufficient power sources for these devices — lithium batteries currently used in cellphones and notebook computers are not powerful enough for devices that would perform several more functions.<sup>33</sup>

While governments have an obvious interest in pervasive computing for reasons of efficiency and economies of scale, it is quite likely to spread on its own, in the same way that the worldwide web has, through individual citizens’ desire for more information about the environments in which they operate.<sup>34</sup> As nanotechnology makes possible smaller and smaller computing devices that have even greater computing capabilities than their larger predecessors, it will become both more economical and efficient to collect, store, process, and distribute vast amounts of information. This will inevitably impact on individual privacy and security.<sup>35</sup>

## The U.S. National Nanotechnology Initiative

The federal government in the United States has long intervened financially in order to boost the development of added value technologies, and in particular, it did so after World War II.<sup>36</sup> The development of the modern computer came about largely as the result of government-funded military research projects during World War II.<sup>37</sup>

In 2003, the U.S. government passed into law the *21st Century Nanotechnology Research and Development Act* (“the Act”),<sup>38</sup> which has as its main purpose to develop commercial uses for nanotechnology. The Act allocates close to \$5 billion in funding from 2004–2008 to the National Nanotechnology Initiative (“NNI”), an initiative that groups together the programs of nine federal agencies, including the National Science Foundation, the National Aeronautics and Space Administration, and the Department of Homeland Security. The federal administration describes the NNI as a top multi-agency research and development priority, and observes that federal spending on nanotechnology research increased by 83% in the previous two years,<sup>39</sup> and was expected to total \$1 billion in the fiscal year 2005.<sup>40</sup>

One of the main goals of the NNI is to fund research and development that will enhance national security in the United States.<sup>41</sup> The vision of the NNI is described as “a future in which the ability to understand and control matter on a nanoscale leads to a revolution in technology and industry”,<sup>42</sup> and towards this end the NNI commits to expediting the discovery, development, and deployment of nanotechnology in order to promote national security, among other things.

National defence and security are seen as areas of cross-cutting application; in pursuit of these goals the NNI is working towards the development of “systems with the speed and capacity to enable command, control, communications, surveillance, reconnaissance, and information dominance”.<sup>43</sup> While some 14 departments and agencies participate to some extent in the development of nanotechnology for national defence and security purposes, as can be expected these drivers are of primary interest to the departments of Homeland Security and Defense.<sup>44</sup>

The Department of Homeland Security has also established a virtual National Cyber Security research and development Center. The Center is the umbrella organization through which the department’s funding for cyber-security research and development activities is distributed.<sup>45</sup> The departments of Homeland Security and Defense are participating in the development of nanotechnology-based systems that will increase the speed of computers, and allow for stable and expanded memory out of their interest in surveillance and communications.<sup>46</sup> Of the 23 federal agencies that participate in the NNI, 11 have research and development budgets for nanotechnology.

Through funding either in whole or in part from the NNI, nano-electro-mechanical sensors have already been developed that can detect and identify even a single molecule of a chemical warfare agent. On the computing front, funding from the NNI has aided in the development of prototype data storage devices, based upon molecular electronics, that have data densities one hundred times that of the highest density commercial devices that are currently available.<sup>47</sup>

## The U.S. National Plan

The *National Plan for Research and Development in Support of Critical Infrastructure Protection*,<sup>48</sup> (“the Plan”) published by The Executive Office of the President, Office of Science and Technology Policy, and the Science and Technology Directorate of the Department of Homeland Security in 2004, underscores the interconnectedness between government, private industry, and individual citizens. As the Plan observes, “critical infrastructures are not just building and structures — they include people and physical and cyber systems that work together in processes that are highly interdependent.”<sup>49</sup>

The Plan outlines one of the primary goals for critical infrastructure protection: to integrate monitoring and surveillance systems with data collection, analysis, and the production of reports. What the authors of the Plan hope this will provide is “real-time situational awareness capability” that would provide what they describe as a “national common operating picture”. They predict that “the heart of the system would be a sensor network that is intelligent, self-monitoring, and self-healing to allow continuous operation for situation monitoring and information transfer.”<sup>50</sup>

The authors of the Plan rightly foresee that this will be made possible if current predictions about the development of computers are realized. Rather than relying upon wires and electricity, computers in the future will be based upon biological processes that use molecules and chemical exchanges. Quantum computers will likely be able to transmit information through the spin of an electron, allowing them to perform vastly more complex functions than today’s computers.<sup>51</sup>

The transformational developments in computing power come at an opportune time for lawmakers in the United States, because, as the authors of the Plan observe, “massive amounts of data will need to be processed and analyzed to selectively filter out background signals in order to detect anomalies or patterns”. All of this data will need to be set in the context of information received from various sensors, and be further analyzed if it is to be of any use to the law enforcement and intelligence community.<sup>52</sup>

Predicting what people will do is a difficult business. However, the Plan states:

The detection of intent involves examining combinations of observations, actions, relationships, and past history in order to accurately sense whether a person, group, or series of events might be the purveyor of or precursor to terrorist events.<sup>53</sup>

The intelligence and law enforcement community may be aided in this respect through the use of so-called “psychologically/physiologically-oriented sensors” that could reveal an individual’s state of mind.<sup>54</sup> The Plan forecasts that:

Intelligent systems will have multiple types of sensors, communication capabilities so they can “talk” to each other, and computing capabilities so they can perform analyses,

compare sensed data and analyses, and learn based on analyses and experience. To be pervasively deployed, such smart sensors need to be low-cost, durable, accurate, self-calibrating, and environmentally adaptable. The sensors and systems of sensors will need to be “taught” to be threat-aware, self-configuring, and self-healing. They may be wired or wireless or a combination of the two — but they must be informationally secure.<sup>55</sup>

These advanced systems will include “smart networks” that communicate with each other and organize tasks so as to collaborate, adjusting themselves to respond to evolving situations.<sup>56</sup> The Plan recognizes the need to incorporate into computer modeling systems as many biometric measurements as possible, in order to reinforce the accuracy of identification and authentication systems.<sup>57</sup>

These research and development efforts are geared towards what is described in the Plan as “dynamic situational control”, essentially, a somewhat ambitious plan to collect vast amounts of data from people, objects, and sensors, analyze this data and then infer actions or intent so as to control the outcome of a given situation:

Dynamic control is the ability to integrate and act on the multiple streams of data collected from people, objects, detectors, and a variety of data systems, such as freight tracking data, airline passenger manifests, Interpol, FBI, local police records, financial information, etc.<sup>58</sup>

Towards the conclusion of the Plan there is some, albeit brief, mention of the necessity of protecting individual and privacy rights. The authors suggest that it will be important to understand the impacts of developing huge databases that contain information about citizens living in the United States and elsewhere.<sup>59</sup>

## Implications of Governmental Use of Nanotechnology in Surveillance

Even if developments in nanotechnology make these new computing capabilities a reality, some challenges remain. The United States government is already implementing, as a research and development priority, multi-database monitoring systems that provide information to law enforcement personnel. The United States Visitor and Immigrant Status Indicator Technology Program, a universal entry-exit program promulgated by the Department of Homeland Security, will collect vast amounts of information about individuals as they arrive and depart from the country. Included among the vast array of information collected will be name and gender, biometric information, citizenship, place of residence and complete address while in the country.<sup>60</sup>

As the authors of the National Plan euphemistically observe, however, “the bulk of these systems will continue to contain legacy technology for which interfacing may be the best that can be done to improve security. These legacy elements are not always capable of integration or intelligent collaboration”.<sup>61</sup> This is a reference to the fact that numerous and diverse databases have been

developed through law enforcement initiatives over the past two decades. Many of these employ incompatible technologies and collect data based upon differing sets of rules, with the result that they cannot simply be combined into a single, searchable database.

The government's desire to collect a wide array of information may reflect the knowledge that individual profiling, which is in essence what is being done, is ineffective if it is done using only raw characteristics such as race, for example. Race alone cannot predict human behaviour; and overreliance upon it can mislead law enforcement authorities and place innocent persons at risk of investigation.<sup>62</sup> Governmental policies involving the racial profiling of Arabs, Muslims, Sikhs and South Asians in the United States since 2001 have failed to uncover substantial terrorist criminal activity against the United States, which points to the failure of race alone as a predictor of violent behaviour.<sup>63</sup> As several commentators have observed, the notion of the "terrorist" that has developed in the political culture in the United States is an intricate formation that includes aspects of race, nationality, and religion. It may unfairly cast members of certain groups as being more likely to commit acts of violence.<sup>64</sup>

Similarly, while the spread of pervasive computing will make it much easier to situate and track the movements of individuals,<sup>65</sup> geographical location alone is not a reliable indicator of future behaviour. So what type of information is the government trying to collect? As many types as possible, it would appear. Persons wishing to cross national borders will be required to provide intimate biological information about themselves, and this information will be stored and used to positively identify them as they move within the U.S. This information will be compared with information from law enforcement officials, border stations, and immigration officials.

A significant reason for the U.S. government's investment in nanotechnology is to collect information and prevent actions that may threaten national security. As recent catastrophes have shown, however, government acting alone is often singularly incapable of reacting swiftly and appropriately. As some have noted, decision-making in the 21<sup>st</sup> century, and the power that goes with it, is de-centralized.<sup>66</sup> Private entities are vertically and horizontally implicated at almost every level of governance, and are involved in even the most demanding business of a nation, such as military engagement.<sup>67</sup> An example of this is a committee convened by the U.S. Directorate for Science and Technology of the Department of Homeland Security. The Directorate has as one of its missions the objective of enhancing the technical capabilities of the department's operations.<sup>68</sup> Another body within the department, the Homeland Security Science and Technology Advisory Committee, identifies research areas that are of potential importance to the security of the United States. In an interesting intersec-

tion between the needs of researchers for funding and the government's need for research into greater computing power, this Committee consists of 20 scientists who are not government employees, and who have established records of distinguished service in relevant fields such as engineering and emergency response.<sup>69</sup>

## Public Engagement in Emerging Nanotechnologies

**I**n addition to the privacy implications developments in nanotechnology may have, there are tangible health and environmental implications. As well, the scientific community's view of public engagement has evolved in recent years. There is a growing realization that it is crucial to consult with, and involve the public in, the development of emerging technologies in order for those technologies to be accepted and in order to properly manage risks. Critics suggest that amidst the large sums that are being spent on nanotechnology research and development, insufficient monies are being allocated to risk management and research into the health and environmental effects of emerging nanotechnologies.<sup>70</sup>

Scholars have recommended a so-called "post-normal" approach for inclusion of members of the public in the development of emerging technologies. They suggest that engaging the public and creating feedback mechanisms will both expand the knowledge base and identify important values and possible areas of conflict.<sup>71</sup> Involving the public in this way transforms individual citizens into a form of "extended peer community" that can help to assess emerging technologies.<sup>72</sup>

The Danes employ a method called the "Danish Consensus Conference" through their Board of Technology, an administrative agency of the government, to create policy statements regarding highly technical issues. The United States Congress employed a similar methodology when it created citizen juries on nanotechnology policy.<sup>73</sup> But to be effective, this has to be more than focus-group testing in a marketing sense. It has to be a feedback loop that takes into account concerns raised and modifies the approach accordingly, in order to build credibility and truly minimize risks.

The challenges of involving the public include the highly technical and complex nature of the terminology — as we have seen with patent issues, terms and concepts in nanotechnology are unlike anything that most members of the public would ever have encountered. Yet, as some authors have pointed out, it is essential that scientists communicate with other members of the public, and become involved in the policy issues that arise with emerging technologies. When they fail to do so, science can become destabilized and overly politicized.<sup>74</sup>

Several commentators on developments in nanotechnology point to the European experience with genetically modified foods, where scientists failed to take into account the general public's mistrust of this technology and the devastating financial impact that that would have on the industry.<sup>75</sup> Private industry, researchers, and government alike have come to realize the importance of informing the public about emerging technologies in a transparent manner that is accountable to public concerns.<sup>76</sup>

Developments in nanotechnology are similar to those in stem cell research in that they involve novel, highly technical scientific developments with potentially enormous societal and political implications. In both cases, the legislative process has not progressed at the same rate as scientific breakthroughs.<sup>77</sup> One of the understandable difficulties with involving legislators and the public is the highly technical nature of nanotechnology applications. The same problem has confounded those rushing to patent new nanotechnology applications. It is difficult for those not intimately involved with emerging nanotechnologies to even imagine some of the new concepts, let alone comprehend them, in order to make informed decisions about their uses. Consider, for example, a patent issued to Cornell University in 2004, for "Entropic Trapping and Sieving of Molecules", a process which retrieves responses to electrical stimuli in order to facilitate the downwards passing of larger molecules while smaller ones remain behind. As has been observed, the behaviour of molecules at the level of nanotechnology runs counter to the way in which we generally understand matter to react.<sup>78</sup>

In the fall of 2005, the United States National Science Foundation provided \$20 million to a Nanoscale Informal Science Education Network that will develop public education exhibits and programs in science museums. Another \$14 million was awarded to universities to allow them to conduct research on the social implications of developments in nanotechnology. As well, the so-called "Societal Dimensions Program Component Area" of the NNI expects to fund \$43 million in 2006 for education and research on the societal implications of nanotechnology, including privacy concerns that may arise from the use of sensors created through nanotechnology.<sup>79</sup>

This may be an indication that the government is borrowing from its experiences in other fields of scientific development. As one researcher observed while testifying before Congress:

... the Human Genome project provides a good model for how an emerging technology can defuse potential controversy by addressing it in the public sphere. Mapping of the human genome carries with it many of the same potential concerns as do other fields of genetic research. The increased availability of genetic information raises the potential for loss of privacy, misuse by the police and insurance companies, and discrimination by employers. The founders of the Human Genome Project did not try to bury

these legitimate concerns by limiting public discourse to the benefits of this new knowledge. Instead, they wisely welcomed and actively encouraged the debate from the outset by setting aside 5% of the annual budget for a program to define and address the ethical, legal and other societal implications of the project.<sup>80</sup>

Potential medical applications of nanotechnology raise numerous interesting questions about which the public will undoubtedly wish to engage. If, for example, as with other emergent technologies, nanotechnology applications are mainly accessible to those with sufficient wealth to afford them in their initial stages, might there be inequalities between persons who have been "enhanced" by nanotechnology versus those who have not?<sup>81</sup> If nanotechnology enhances a person's capabilities, *quaere* whether there will be any distinction between personal capabilities and individual identity.<sup>82</sup> Organizations that promote the interests of transhumanists, individuals who believe that technology may be used to enhance human beings, press for less regulation and greater investments in nanotechnology.<sup>83</sup>

Some commentators have described a new "dignitarian view", which, along with utilitarian and human rights perspectives, forms an emerging triangle in debates about bioethics.<sup>84</sup> The dignitarian view informs the *Preliminary Draft Declaration on Universal Norms on Bioethics*, published by the International Bioethics Committee of the United Nations Educational, Scientific and Cultural Organization ("UNESCO") and promotes the development of scientific research within a framework that respects human dignity.<sup>85</sup> The International Declaration on Human Genetic Data,<sup>86</sup> which is principally concerned with the collection, storage and use of human genetic data for research purposes, specifically provides that human dignity must be protected.<sup>87</sup> The Declaration recognizes that an individual's identity cannot be reduced to genetic characteristics, and that it is a complex mixture of environmental, social and cultural factors, including an aspect of freedom.<sup>88</sup>

Whereas human rights concerns may be largely addressed through a requirement to obtain informed consent, dignitarians would argue that there may be situations where, even with informed consent, a given biotechnology attacks fundamental human dignity. An example of this would be an application of biotechnology that fundamentally altered what is understood to be an inherently human trait.<sup>89</sup> What is interesting about the dignitarian point of view is that the giving of consent does not end the matter — there is a higher value of human dignity that it would seek to protect.<sup>90</sup>

Another challenge, quite apart from the privacy implications of nanotechnology, is the effect that minuscule matter, or nanoparticles, may have upon human health. Some scientists suggest that nanoparticles may have adverse effects upon human health for two reasons. Early laboratory studies suggest that nanoparticles, or bits of matter on the nanoscale, may enter the body more easily than larger bits of matter. As well, nanotechnology

allows molecular structures to reproduce, and potentially, to self-assemble into more complex structures. This capacity to replicate and proliferate is of concern if it involves matter that is harmful to human health or the environment.<sup>91</sup> Early studies suggest that nanoparticles not only enter the body easily, they may pass through bodily tissues from one area of the body to another, causing inflammation and damaging cells.<sup>92</sup> Not much is known, however, about the toxicity of nanoparticles when inhaled or otherwise taken into the body.<sup>93</sup> In the absence of a regulatory framework, the U.S., companies developing nanotechnology applications may offer generic information about the properties of their products to the Environmental Protection Agency. This would in turn allow those companies to advertise their collaboration with the Environmental Protection Agency as a way of mitigating public concerns about their products.<sup>94</sup>

## Conclusion

Developments in nanotechnology may both facilitate surveillance and increase the power to process information obtained through surveillance.<sup>95</sup> These developments in technology may have an effect on traditional notions of privacy: if it becomes easier and less expensive to gather and use information about people, it may become more common, and eventually, more generally accepted.<sup>96</sup> The evolution of pervasive computing, with various information networks connected to many — and possibly invisible — sensors, suggests that traditional notions of privacy and private and public spaces may need to be re-defined.<sup>97</sup>

So what does all of this do for the U.S. government's goal, described above, of foreseeing and averting threats to national security? The U.S. government, through its Department of Homeland Security is, in a sense, engaging in a vast foresighting exercise. Distinct from forecasting, which passively tries to predict future events, foresighting is based on the notion that there are many possible outcomes in the future, and that it may be possible to intervene and affect these results.<sup>98</sup>

The information that will be collected is raw data, mere information that cannot be characterized as security "intelligence" unless, and until, it becomes an indicator of a potential threat. Given the problems with compatibility of the existing technical infrastructure, it is unlikely that this type of sophisticated analysis will occur at any point in the near future.

More fundamentally, however some of the principles underlying the development of a massive database of biological and other personal information appear to be based upon traditional notions of scientific theory. The model outlined in the National Plan presupposes that biological, geographical, and other information will be collected, and that analysis of this data will provide a form of early warning system that will enable the government to intervene and prevent what it conceives of as harmful events.

Physicists, mathematicians, microbiologists and other scientists are developing a field of study known as "complex adaptive systems", which are inherently subjective, nonlinear, nonpredictive, and mutable.<sup>99</sup> The behaviour of a given group of human beings can be characterized as a complex adaptive system which, while grounded in biology, is by no means locked in by it. Human systems tend to exhibit emergent behaviour when they exist in a realm between chaos and order, where there is some conflict but not debilitating conflict.<sup>100</sup>

In building the databases described in this paper, the U.S. government appears to have failed to take account of the fluid nature of human behaviour and evolution. Human beings, both as individuals and in the communities that they form, are complex adaptive systems. If nanotechnology will soon make pervasive computing a part of our daily lives, then individuals may use it as well to gain contextual information about their environments and to modify their behaviour accordingly.<sup>101</sup> It remains to be seen whether the huge financial investment in a massive surveillance system will actually assist the U.S. government in predicting and averting threats to national security.

## Notes:

<sup>1</sup> Lisa Madelon Campbell, "Rising Governmental Use of Biometric Technology: An Analysis of the United States Visitor and Immigrant Status Indicator Technology Program" (2005) 4 C.J.L.T. 99.

<sup>2</sup> Robert D. Pinson, "Is Nanotechnology Prohibited by the Biological and Chemical Weapons Conventions?" (2004) 22 Berkeley J. of Int'l Law 279 at 282.

<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 iii.

<sup>4</sup> Francisco Castro, "Legal and Regulatory Concerns Facing Nanotechnology" (Fall, 2004) 4 Chicago-Kent J. of Intellectual Property 140 at 140.

<sup>5</sup> 1<sup>st</sup> ed, (New York: Anchor Books, 1986).

<sup>6</sup> Wayne C. Jaeschke & Kimberly A. Kluge, "Innovating from Pumps to Genes into the 'Nano-dimension': The Legal Consequences of the Insatiable Urge to Build a Better Mousetrap" (2004) 22 Del. Law. 38 at 40.

<sup>7</sup> K. Eric Drexler, "Nanotechnology Summary" in 1990 *Encyclopedia Britannica Science and the Future Yearbook*, 162 at 163 as cited in Glenn Harlan Reynolds, "Nanotechnology and Regulatory Policy: Three Futures" (Fall, 2003) 17 Harvard J. of Law & Technology 179 at 180.

<sup>8</sup> Office of the Press Secretary, News Release, "President Bush signs Nanotechnology Research and Development Act into Law" (3 December 2003), online: The White House <<http://www.whitehouse.gov/news/releases/2003/12/20031203-7.html>>.

- <sup>9</sup> Terry K. Tullis, "Application of the Government License Defense to Federally Funded Nanotechnology Research: The Case for a Limited Patent Compulsory Licensing Regime" (2005) 23 UCLA L. Rev. at 283.
- <sup>10</sup> Castro, *supra* note 4 at 141.
- <sup>11</sup> Pinson, *supra* note 2.
- <sup>12</sup> Meridian Institute, "Nanotechnology and the Poor: Opportunities and Risks — Closing the Gaps Within and Between Sectors of Society" (January 2005) online: <<http://www.nanoandthepoor.org>>.
- <sup>13</sup> Tullis, *supra* note 9.
- <sup>14</sup> Dana E. Nicolau, "Challenges and Opportunities for Nanotechnology Policies: An Australian Perspective" (2004) 1:4 Nanotechnology L. & Bus. 446 at 459.
- <sup>15</sup> *Ibid.* at 460.
- <sup>16</sup> U.S., Nanoscale Science, Engineering, and Technology Subcommittee Committee on Technology, National Science and Technology Council, *The National Nanotechnology Initiative — Research and Development Leading to a Revolution in Technology and Industry* (2006) at i.
- <sup>17</sup> Karen Florini *et al.* "Nanotechnology: Getting it Right the First Time" (2006) 6:3 Sustainable Development L. & Policy 46 at 51.
- <sup>18</sup> Office of Science and Technology Policy, Executive Office of the President, News Release, "Nanoscale Scientific and Engineering Research and Development Extend Frontiers of Scientific Knowledge, Lead to Significant Technological Advances — Supplement to President's FY 2004 Budget Released Today" (17 October 2003).
- <sup>19</sup> *Supra* note 16 at 35.
- <sup>20</sup> Steve Jurvetson, "Transcending Moore's Law with Molecular Electronics and Nanotechnology", (2004) 1:1 Nanotechnology Law and Business 70 at 72.
- <sup>21</sup> Thomas A. Kalil, "Next Steps for the National Nanotechnology Initiative" (2004) 1:1 Nanotechnology L. & Bus. 55 at 59.
- <sup>22</sup> Jurvetson, *supra* note 20 at 88.
- <sup>23</sup> Lawrence Gasman, "Making Powerful Information Technology Available Everywhere: Nanotech and the Next Wave: Pervasive Computing" online: Foresight Nanotech Institute, <<http://www.foresight.org/challenges/it.php>>.
- <sup>24</sup> *Supra* note 8.
- <sup>25</sup> "Where Nanotechnology & The Computer Industry Meet — Shrinking the PC" *Computer Power User* 2:3 (March, 2002) 56.
- <sup>26</sup> Stephen Lovgren, "Computer made from DNA and Enzymes" *National Geographic News* (24 February 2003), online: National Geographic News <[http://news.nationalgeographic.com/news/2003/02/0224\\_030224\\_DNAcomputer.html](http://news.nationalgeographic.com/news/2003/02/0224_030224_DNAcomputer.html)>
- <sup>27</sup> National Technology Initiative, "Applications/Products" online: National Technology Initiative <<http://www.nano.gov/html/facts/appsprod.htm>>.
- <sup>28</sup> Jerry Kang & Dana Cuff, "Pervasive Computing: Embedding the Public Sphere" 62 Wash. & Lee L. Rev. 93 (2005) 93 at 99; also available at <<http://ssrn.com/abstract=626961>>.
- <sup>29</sup> *Ibid.* at 112.
- <sup>30</sup> *Ibid.* at 99.
- <sup>31</sup> *Supra* note 8.
- <sup>32</sup> Pinson, *supra* note 2.
- <sup>33</sup> Gasman, *supra* note 23.
- <sup>34</sup> Kang & Cuff, *supra* note 28 at 101-102.
- <sup>35</sup> Fiona N. Moore, "Implications of Nanotechnology Applications: Using Genetics as a Lesson" (2002) 10:3 Health L. Rev. 9.
- <sup>36</sup> Nicolau, *supra* note 14 at 458.
- <sup>37</sup> Mark A. Lemley, "Patenting Nanotechnology" June 2005, Stanford Law School, John M. Olin Program in Law and Economics, Working Paper No. 304, at Social Science Research Network Electronic Paper Collection: <<http://ssrn.com/abstract=741326>>, at page 8.
- <sup>38</sup> 15 U.S.C.A. §7501-7509.
- <sup>39</sup> *Supra* note 8.
- <sup>40</sup> *Supra* note 3 at iii.
- <sup>41</sup> *Ibid.* In his covering letter to the Strategic Plan, John H. Marburger, Director of the Executive Office of the President, Office of Science and Technology writes that, since its inception in 2001, the NNI has sought to enhance national security, among other things.
- <sup>42</sup> *Ibid.* at 1.
- <sup>43</sup> *Ibid.* at 20.
- <sup>44</sup> *Ibid.* at 20.
- <sup>45</sup> U.S., The Executive Office of the President, Office of Science and Technology Policy & The Department of Homeland Security, Science and Technology Directorate, *The National Plan for Research and Development in Support of Critical Infrastructure Protection* (Washington, D.C., 2004) at 8.
- <sup>46</sup> *Supra* note 3 at 21.
- <sup>47</sup> National Nanotechnology Initiative, *Nanotechnology: from Imagination to Reality*, online: National Nanotechnology Initiative <[http://www.nano.gov/html/res/fy04-pdf/fy04%20-%20small%20parts/NNI.FY04\\_D\\_intro.pdf](http://www.nano.gov/html/res/fy04-pdf/fy04%20-%20small%20parts/NNI.FY04_D_intro.pdf)>
- <sup>48</sup> *Supra* note 45.
- <sup>49</sup> *Ibid.* at 2.
- <sup>50</sup> *Ibid.* at 13.
- <sup>51</sup> *Ibid.* at 15.
- <sup>52</sup> *Ibid.* at 24.
- <sup>53</sup> *Ibid.* at 26.
- <sup>54</sup> *Ibid.* at 26.
- <sup>55</sup> *Ibid.* at 27.
- <sup>56</sup> *Ibid.* at 59.
- <sup>57</sup> *Ibid.* at 38. Biometric identifiers are physical and behavioral measurements or characteristics that include fingerprints, hand geometry, facial features and deoxyribonucleic acid (DNA).
- <sup>58</sup> *Ibid.* at 41.
- <sup>59</sup> *Ibid.* at 67.
- <sup>60</sup> Susan Martin & Philip Martin, "National Security Discussion: International Migration and Terrorism: Prevention, Prosecution and Protection" (2004) 18 Geo. Immigr. L. J. 329, at 333.
- <sup>61</sup> *Supra* note 45 at 71.
- <sup>62</sup> Martin & Martin, *supra* note 60 at 337.
- <sup>63</sup> Thomas M. McDonnell, "Targeting the Foreign Born by Race and Nationality: Counter-Productive in the 'War on Terrorism?'" (2004) 16 Pace Int'l L. Rev. 19, at 8.
- <sup>64</sup> Margaret Chon & Donna E. Arzt, "Judgments Judges and Wrongs Remembered: Examining the Japanese American Civil Liberties Cases on their Sixtieth Anniversary: Walking While Muslim" (2005) 68 Law & Contemp. Probs. 215.
- <sup>65</sup> Kang & Cuff, *supra* note 28 at 103.
- <sup>66</sup> Robert J. Rhee, "Catastrophic Risk and Governance after Hurricane Katrina: A Postscript to Terrorism Risk in a Post-9/11 Economy" (2006) 38 Ariz. St. L. J. 581 at 603.
- <sup>67</sup> *Ibid.*
- <sup>68</sup> Department of Homeland Security, online: <<http://www.dhs.gov/index.shtm>>
- <sup>69</sup> *Ibid.*
- <sup>70</sup> Florini *et al.* *supra* note 17 at 51-52.
- <sup>71</sup> Michael D. Mehta, "Regulating Biotechnology and Nanotechnology in Canada: A Post-Normal Science Approach for Inclusion of the Fourth Helix" (Paper presented at the International Workshop on Science, Technology and Society: Lessons and Challenges, National University of Singapore, 19 April 2002) [unpublished] at 7-8.
- <sup>72</sup> *Ibid.* at 22.
- <sup>73</sup> Beth Simone Noveck, "The Future of Citizen Participation in the Electronic State" (2004) 1:1 J. of Law and Policy for the Information Society 1 at 12.
- <sup>74</sup> Gregory N. Mandel, "Technology Wars: the failure of democratic discourse" (2005) 11 Mich. Telecomm. & Tech. L. Rev. 117.
- <sup>75</sup> Bryn Williams-Jones, "A Spoonful of Trust Helps the Nanotech Go Down" (2004) 12:3 Health L. Rev. 10.
- <sup>76</sup> *Ibid.* See also Emmanuelle Schuler, "A Prospective Look at Risk Communication in the Nanotechnology Field" (2004) 12:3 Health L. Rev. 28.

<sup>77</sup> William P. Cheshire, Jr., "Small Things Considered: the Ethical Significance of Human Embryonic Stem Cell Research" (2005) 39 *New Eng. L. Rev.* 573.

<sup>78</sup> Jaeschke & Kluge, *supra* note 6 at 80.

<sup>79</sup> National Nanotechnology Initiative, "Societal Dimensions" online: <[http://www.nano.gov/html/society/home\\_society.html](http://www.nano.gov/html/society/home_society.html)>.

<sup>80</sup> Testimony of Vicki Colvin, Director, Centre for Biological and Environmental Nanotechnology, before the House Committee on Science, 108<sup>th</sup> Congress (2003) in regard to *21st Century Nanotechnology Research and Development Act* of 2003. Also available online: House Committee on Science <<http://www.house.gov/science/hearings/full03/apr09/colvin.htm>>.

<sup>81</sup> R. George Wright, "Personhood 2.0: Enhanced and Unenhanced Persons and the Equal Protection of the Laws" (2005) 23 *Quinnipiac L. Rev.* 1047.

<sup>82</sup> *Ibid.*

<sup>83</sup> Edna F. Einsiedel & Greg McMullen, "Stakeholders and Technology: Challenges for Nanotechnology" 12:3 *Health L. Rev.* 5.

<sup>84</sup> Roger Brownsword, "Stem cells and Cloning: where the Regulatory Consensus Fails" (2005) 39 *New Eng. L. Rev.* 535 at 538.

<sup>86</sup> United Nations Educational, Scientific and Cultural Organization (UNESCO), International Declaration on Human Genetic Data (16 October 2003), online: UNESCO <<http://portal.unesco.org>>.

<sup>86</sup> United Nations Educational, Scientific and Cultural Organization (UNESCO), International Declaration on Human Genetic Data (16 October 2003), online: UNESCO <<http://portal.unesco.org>>.

<sup>87</sup> *Ibid.* at preamble.

<sup>88</sup> *Ibid.* at Article 3.

<sup>89</sup> Brownsword, *supra* note 84 at 553.

<sup>90</sup> *Ibid.*

<sup>91</sup> Albert C. Lin, "The Unifying Role of Harm in Environmental Law" (2006) 2006 *Wis. L. Rev.* 897.

<sup>92</sup> Jennifer Sass, Patrice Simms & Elliott Negin, "Nanotechnologies: The Promise and the Peril" (2006) 6:3 *Sustainable Development Law & Policy* 11, at 11.

<sup>93</sup> *Ibid.*

<sup>94</sup> *Ibid.*, at 13.

<sup>95</sup> Chris MacDonald, "Nanotechnology, Privacy and Shifting Social Conventions" (2004) 12:3 *Health L. Rev.* 37.

<sup>96</sup> *Ibid.*

<sup>97</sup> Davis Baird & Tom Vogt, "Societal and Ethical Interactions with Nanotechnology ('SEIN') — An Introduction" (2004) 1:4 *Nanotechnology Law and Business* 391 at 394.

<sup>98</sup> Ian Kerr & Goldie Bassie, "Building a Broader Nano-network" (2004) 12:3 *Health L. Rev.* 57.

<sup>99</sup> Scott H. Hughes, "Understanding Conflict in a Postmodern World" (2004) 87 *Marq. L. Rev.* 681 at 683.

<sup>100</sup> *Ibid.* at 684.

<sup>101</sup> Kang & Cuff, *supra* note 28.