ACADEMIA ENGELBERG

2nd Dialogue on Science – 15 - 17 October 2003
in Engelberg, Switzerland

Science and Trust in Conditions of Uncertainty

Kathinka Evers, Dr., Assoc. Professor,
Research Director, University of Uppsala,
Department of Ethics in Biomedicine/
Institute of Public Health, Sweden

Contact:
Uppsala Science Park, SE-75184 Uppsala
email: kathinka.evers@bioethics.uu.se

I have been asked to speak on the theme of science and trust in a way that helps set a general stage for subsequent discussions on pervasive computing1. The topic is of course enormous, and in this presentation I shall only address a few points that appear particularly able to provoke social unease and mistrust concerning certain aspects of scientific and technological advance.

1. Trust as an epistemic or as a moral attitude

Trust becomes relevant in the face of possible abuse or misuse of some capacity or power. From a scientific point of view, the primary form of trust is epistemic (i.e., knowledge-related); it concerns objective accuracy, truth and justification in a way that can be, but that is not necessarily, moral. Those who engage in science need to have confidence in the integrity of their colleagues' results. False or unjustified theories can block the development of knowledge, and even lead to regress. When, say, a research team comes up with false or unjustified conclusions, the question arises, why they have done so; whether their mistakes evoke moral problems. The history of science is full of errors, and it is important to bear in mind that some, but not all errors, raise moral issues.

Public debates over science and trust concern moral rather than epistemic trust. As a rule, people are not overly critical about the epistemic adequacy of scientific pursuits as such: there appears to be a fair level of trust that most scientists at least try to do a good job, if left to their own devices. The serious suspicions and worries rather concern the temptations and pressures to which scientists are subjected, and the use that decision-makers make of their results. Rapid developments in science and technology that are difficult to understand, let alone control, easily create conditions of uncertainty that, if they are not clarified, or counterbalanced, provide fertile grounds for mistrust and fears of possible abuse.

Progress in science depends on public trust, in the moral sense. Trust in the integrity of science is vital to ensure societal support, and also in part because participation, e.g., in statistical enquiries or experiments, is based upon informed consent for which trust is a normal prerequisite. Public investment in science and technology is predicated upon the expectation of some return to society, which is an essential aspect of producing and meriting public trust. A central question thus becomes: What returns might inspire and merit, or destroy public confidence?

[1] Academia Engelberg, Dialogue on Science and Trust and Pervasive Computing, October 15-17, 2003, Engelberg, Switzerland.

2. Public trust and pervasive computing

Science and technology are major forces of socio-economic change, but they are a mixed blessing. On the one hand, scientific and technological advances have resulted in great benefits for humankind, such as medical care, means of rapid communication, etc. On the other hand, "scientific progress has made it possible to manufacture sophisticated weapons…of mass destruction" and has "also led to environmental degradation and technological disasters"2. Furthermore, the benefits of development, such as access to medical care, are distributed on our globe with profound inequality3, whilst degradation, notably environmental, is typically suffered worst by those who are racially, sexually and economically disadvantaged, and who rarely enjoy the beneficial side of the same coin. In the world we have created, largely by the aid of science and technology, we reduce a steadily growing majority of the earth's population to a life without either dignity or hope. Since this is primarily a result of human decisions, it is perhaps not surprising if people in large parts of the world do not conceive of science as being essentially a benefactor of humanity, nor readily associate science with the classical quest of developing a more enlightened civilisation. A general unease appears to be spreading now, both within and beyond scientific communities, concerning the direction in which human societies are heading.

In order to understand this unease and create conditions for trust, it is important to understand towards what, or whom, mistrust primarily is directed. Here there are important political and economic factors to consider. Public trust can only be expected to develop if there is a fair amount of transparency that permits insight into the processes of development, and relatively clear standards for accountability when things go wrong. The public expects the scientific communities to "avoid unethical exploitation of their professional status by endorsement of misleading or fraudulent advertising or product certification…"4. False or misleading arguments spread to increase economic profits and gain political advantages from scientific and technological developments constitute (when disclosed) a major obstacle to the creation of trust. For example, "consider the oft-quoted myth that the usage of mobile telephones would offer the poor in developing countries crucial information that would help them liberate themselves and develop. The story is nice but problematic: 5 minutes of communication in Africa often cost the equivalent of a day's salary".5

[2] The Declaration on Science and the Use of Scientific Knowledge adopted by the World Conference on Science 1999, 3§. Nanotechnology illustrates well this mixed blessing. Suggested uses of this new technology are potentially both beneficial, notably in the area of medicine, and destructive, e.g., the fabrication of a mini-bomb the size of a pencil, capable of erasing entire cities (cf., e.g., CORDIS focus, No 224, June 30, 2003, pp. 1-2).
[3] For example, whilst there are 30 million HIV-positive people in Africa, 99% of the people who have access to advanced medication live in developed countries Cf., e.g., Germán Velásquez & Pascale Boulet (1999), and Germán Velasquez (2003, p. 26).
[4] Guidelines 7 and 8 of the International Union of Food Science and Technology's (IUFoST) 'Guidelines of Professional Behaviour'.
[5] Eric Guichard (2003).

Today, two much debated and closely related values that both have special relevance to pervasive computing are personal integrity and democracy. It is sometimes alleged that "Computer networks, unlike other mass media, have a truly global character" 6 and that "Even more distant developing countries can fully participate in cyberspace and look forward to new opportunities offered by global networks…"7 This happy state is also supposed to guarantee political freedom to develop: "…the net constitutes the only realm of freedom in many non-democratic countries. Also the opportunities which the Internet offers to commerce guarantee its freedom: no country could afford losing this competitive advantage."8

Here we have false arguments coupled with an outstanding naivety. To begin with, it is not true that developing countries can fully participate in cyberspace; economic and social factors, notably, hinder this. In developing countries, the poor do not participate in cyberspace, which is reserved for a small minority of wealthy citizens. Secondly, the development of computer networks can serve tyranny as well as freedom, and possibly even better. Without knowledge to evaluate information received, people become passive recipients and all the more easy to manipulate9. There are few more potent threats against an open and democratic society than the development of pervasive surveillance and control over citizens, for which there can scarcely be a more effective method than pervasive computing.

In many countries that are at least formally democratic, computer networks appear to pose a potent threat to personal integrity and political freedom. For example, the Echelon interception system, described as "a global system for the interception of private and commercial communications"10 is a network of interception stations launched by the United States with the aid of strategic partners (Britain, Australia, New Zealand and Canada) which enables them to intercept phone-calls, fax and electronic mails (anything using electromagnetic energy) over the entire globe. The system was launched in the 70s, during the Cold War. After the Cold War, the Echelon surveillance increased with Europe as a prime target. The European Parliament has reacted negatively on this surveillance, not least since Britain could in principle be acting as a double-agent engaging in, for instance, commercial spying on its European partners.11

What makes public trust particularly difficult to achieve in this domain, is that people regularly discover that they have been misled. The existence of Echelon was long denied. When that became

[6] Krystyna Gorniak-Kocikowska (1996).
[7] Jacek Sojka (1996, p. 192).
[8] Ibid., p. 198.
[9] A point I owe to Alberto Casco, in discussion of this paper.
[10] European Parliament, Temporary Committee on the ECHELON interception system, report of May 18 2001 (rapporteur: Gerhard Schmid).
[11] A web-site called 'Echelonwatch' highlights news around the world, valuable for those who are interested in checking the ongoing debate, http://archive.aclu.org/echelonwatch/highlights.html

a non-option, its use was declared very limited, especially in the case of partner countries. For example, in the 80's, the citizens of New Zealand were falsely led to believe that their country was safely cut off from the NSA (U.S. National Security Agency) espionage, whereas, in reality, the country's cooperation with NSA had been increased and the use of Echelon accelerated, aided by the press leading a campaign of disinformation.12 It is doubtful that the tax-payers of the United States are fully aware of the gigantic sums their government spends on Echelon, and if informed, they might well prefer a different use of their tax-revenues, such as investments in education and health care.

Assuming that neither the existence nor the global coverage of Echelon can credibly be denied, a third attempt to defend Echelon against criticism and mistrust is to claim that it is not used to spy on private or commercial communications. The partner countries are not, by that argument, interested in personal data of foreign citizens, nor in commercial communications, but only in national security and related issues, such as terrorism.

A point worth noting in that context is that for the last eighteen months, allegedly, "[t]he U.S. government has been buying personal data on millions of residents in several countries...A Georgia-based data-collecting company named Choice Point has acknowledged that it's been quietly compiling information on tens of millions of ordinary Latin Americans without their consent or knowledge – and the firm has been selling the data to U.S. government agencies for the last eighteen months."13 Mexico has now forced them to stop, but the firm is "prompting authorities in Argentina, Brazil, Nicaragua and Colombia to open formal probes". The information is alleged to include "confidential details about private citizens, including their outstanding debts, bank accounts and homeownership records", and in Colombia "Choice Point seems to have bought the entire national voter registry". Roughly "Thirty million Colombians have been placed in the databases of U.S. agencies".14

Some might consider such procedures to be legitimate to promote what they like to refer to as the "free world", whilst others would regard that description as a perversion of the concept freedom. The point I wish to make here, however, is not evaluative but descriptive.

Pervasive, computerised and secret political control over national and foreign citizens cannot be characterised as compatible with democratic governance and civil rights of freedom by any justifiable definition. To the extent that phenomena like the Echelon espionage and governmental data

[12] Cf., e.g., Philippe Rivière (1999) and Nicky Hager (1996).
[13] Joseph Contreras (2003, p. 35).
[14] Ibid. Quote from Colombian congress man Gustavo Petro, who publicly accuses this to violate privacy status.

collection on foreign citizens exist and are allowed to develop, the pervasiveness of computing seems well able to pose a threat to political freedom and civil rights.

3. Transparency, accountability and control as prerequisites for public trust

The social and moral dilemmas to which some scientific and technological developments, such as pervasive computing, give rise contain complex political, economic and legal dimensions that cannot be ignored lest public trust be neither inspired nor merited. We cannot escape the conditions of uncertainty that rapid advances in science and technology create. However, to the extent that they provide grounds for mistrust, those can constructively be counterbalanced without hindering these advances; for example, by offering:

- publicly accessible and transparent analyses of the risks involved;
- clear standards of accountability;
- assurance of socio-political control of the new knowledge and technologies in question.

The development should be controlled and directed by governments and institutions in co-operation. Within an international (e.g., European) perspective, the construction of an international (European) body of control could be valuable in order to ensure, for example, that projects that are considered unethical and inadmissible by national regulations are not simply moved to another country where regulations are, if not officially then at least in practice, more permissive. There would have to be clear standards for accountability in order to render such a body legitimately convincing. Such transparency, accountability, control and firmness of direction would most probably help gain public trust. In any case, it is a prerequisite for its justification.

References

1. Bynum and Rogerson: 1996, Global Information Ethics, Opragen Publications.
2. Contreras, Joseph : 2003, ‘Those Prying Eyes’, Newsweek, July 14, 2003.
3. CORDIS focus, No 224, June 30, 2003.
4. European Parliament, Temporary Committee on the ECHELON interception system, report of May 18 2001 (rapporteur: Gerhard Schmid).
5. Gorniak-Kocikowska, Krystyna: 1996, ‘The Computer Revolution and the Problem of Global Ethics’, in Bynum and Rogerson (1996, 177-90).
6. Guichard, Eric: 2003, ‘ICT : wrong theories, real questions. Myths in the ICT discourse’. Presentation at the 53d Pugwash Conference on Science and World Affairs – Advancing Human Security: The Role of Technology and Politics. 17-21 July 2003; Halifax, Nova Scotia, Canada.
7. http://barthes.ens.fr/pugwash2003/Halifax-Guichard.en.html

8. Hager, Nicky: 1996, Secret Power. New Zealand's Role in the International Spy Network, Craig Potton Publishing, Nelpson, New Zealand. Distributed in the U.S. by Covert Action Quarterly, Washington DC.
9. International Council for Science (ICSU) and UNESCO: 'The Declaration on Science and the Use of Scientific Knowledge' adopted by the World Conference on Science, Budapest, Hungary, 1999.
10. International Union of Food Science and Technology (IUFoST): 'Guidelines of Professional Behaviour'.
11. Rivière, Philippe : 1999, 'Le système Echelon', Le Monde Diplomatique, July 1999, pp. 40-42.
12. Velásquez, Germán: 2003, 'Hold-up sur le médicament', Le Monde Diplomatique, July 2003.
13. Velásquez, Germán and Boulet, Pascale: 1999, Mondialisation et accès aux médicaments. Perspectives sur l'accord Adpic de l'OMC. WHO, Genève, 1999.
14. Sojka, Jacek: 1996, 'Business Ethics and Computer Ethics: The View from Poland' in Bynum and Rogerson (1996, 191-200).