

The following are some issues that come up when the issue of high performance computing is discussed. I do not intend to take a personal stand on these issues of ethics, public policy, and professional responsibility. I encourage you to look these topics up on the web and through other means. The words in parentheses can be used as keywords for a search.

Many of these topics have suddenly become much more high-profile. Opinions may be changing after 11 September. National needs may also be different now from what they were.

Other topics can also be discussed.

1. **United States Constitution:** (US Constitution, Bill of Rights, First Amendment, Fourth Amendment, “clear and present danger”) Probably much more should be said, but no more ought to be needed to be said.
2. **Export controls:** (export controls, ITAR, COCOM, nuclear proliferation) During the Cold War there were many manufactured items that could not be exported to certain countries. Supercomputers have been on the banned list for some time. One celebrated case involved the US Government forbidding the sale of a Cray supercomputer to India. The rationale has been that it is not possible to run a nuclear weapons program without the use of high end computers. Machines that have been permitted to be sold have been sold with restrictions that they be used for peacetime purposes (nuclear power, not nuclear weapons). Many US industries have chafed at these restrictions, claiming that this hurts business.

On the other hand, what is in fact exportable? What actually constitutes “export” in an electronic world?

3. **Controls on cryptography:** (export controls, ITAR, COCOM, CLIPPER chip, LEAF)

Similar export restrictions have existed on the distribution outside the US of information about cryptographic methods. George Davida had a patent declared classified. The CLIPPER chip was proposed as a standard, then withdrawn.

One issue that continues to arise is the question of whether cryptographic methods and devices should contain a back door so as to allow law enforcement officials to circumvent the cryptography. On the CLIPPER chip, this was the LEAF (Law Enforcement Access Field), which in an early draft was inappropriately referred to as the Law Enforcement Access Key.

4. **Industrial policy:** (Industrial policy) The market for very high end computers has dropped significantly since the end of the Cold War. The perceived need for a continued progression of Cray-like computers has diminished; some computing needs are met with cheaper distributed machines of a Beowulf nature, and some may be met with “the Grid” of the future. Nonetheless, there are those who argue that huge SMP machines are necessary for solving some problems, and that some of those problems are so important that the US cannot afford not to be able to solve them.

With the decline in the demand by the DoD for high end machines,

the production of high end machines has dropped off significantly. To provide for a continued progression of Cray-class SMP machines would require something like a subsidy from the USG. Should the USG target specific companies or industries for subsidy? Is this an appropriate thing? Purist believers in the capitalist marketplace say no.

5. **Personal privacy:** (data mining, identity theft) Who owns your data? To what extent is it appropriate that your buying habits be available and usable by commercial firms or become public information?

To what extent should your entire electronic identity be known to the outside world? To what extent should you be permitted to be secure in your home from unwarranted electronic search and seizure? Should you be permitted to use cryptography to secure your communications with others? (This is forbidden in France, for example.)

6. **Applications:** (Union of Concerned Scientists, Physicians for Social Responsibility) There are those who argue that it is improper (immoral? unethical?) for scientists and engineers to work on such things as weapons of mass destruction, chemical or biological agents, or the like. In the world of computing, certainly the development of programs for nuclear weapons design comes under this umbrella, as does work on methods for detailed surveillance and monitoring of individual actions. As the record of the USG during the Vietnam and civil rights era shows, the USG has in the not so distant past spied on US citizens and has used its intelligence capability to attempt to discredit those who have exercised their Bill of Rights freedoms in ways felt by certain

government officials to be politically damaging.

One of the great questions for society is how to deal with technology. Not just in computers but in nearly all aspects of technology it has become *possible* to do things that we as a society or as many societies don't know yet whether we *ought* to be doing. Our use of technology in law enforcement or defense can also become abuse if it is turned against others for inappropriate political reasons. Is it acceptable to work on nuclear weapons design? cryptography? surveillance technologies? genetic engineering?

Where do we draw the line?

How do we control those with power to see that they do not abuse it?