NEWSLETTER ON PHILOSOPHY AND COMPUTERS

FROM THE EDITOR, Jon Dorbolo

FROM THE CHAIR, Robert Cavalier

EVENT HANDLERS

Marvin Croy
“Conversation with Pat Suppes”

WEBSITE SEARCH

Kenneth Einar Himma
“The Radical Academy: Philosophy, Politics, and the Human Condition”

COMPUTING ETHICS

Douglas Birsch
“Endgame: Ethics and Values in America and Morality and Machines”

TEACHING IN CYBERSPACE

Rob Brady, Program Author
“LogicWorks: The Next Generation”

John P. Buerck, Director, Donna J. Werner, Program Coordinator, and Asai Asaithambi, Chairperson
“Integrating Ethics Into a Computer Science and Technology Curriculum: Challenges, Accomplishments, and New Opportunities”

PLATFORM

Jon Dorbolo
“Power in Terror”
The same issue arises with uses of information technology in the process of learning that subject matter cannot be equated. The features of a subject matter and the features of learning even elementary lessons is itself a massively complex to the simplicity of the learning task. Yet, as Suppes notes, simplicity of the subject-matter to be learned as an analogue (Suppes, 1979, p.42). It is tempting for teachers to regard the unbounded complexity in terms of learning and performance.” (Suppes, 1979, p. 44). Not only has the problem of intellectual interaction not been solved, it is not often clearly addressed now-a-days. Patrick Suppes sets the standard for what serious attention to this problem will be like.

Professor Patrick Suppes is Professor Emeritus at the Center for the Study of Language and Information, Stanford University. Since receiving his Ph.D. at Columbia University in 1950, Prof. Suppes has won numerous honorary degrees and awards; the most recent being the 2002 Barwise prize. At that event, Marvin Croy recorded a conversation with Patrick Suppes. Their conversation is presented in this issue.


2003 Computing and Philosophy Conference
Oregon State University will host the 2003 CAP conference. Complementing the excellent program will be Western Oregon’s late summer weather. Old growth forest trips and the wild Oregon coast are just nearby. Consider making this trip a family event. See http://oregonstate.edu/groups/cap for details and contact Jon Dorbolo (Jon.Dorbolo@orst.edu) 541.737.3811 with questions. The salmon will be on the grill - - see you there.
FROM THE CHAIR

Robert Cavalier
Carnegie Mellon University
rc2z@andrew.cmu.edu

Please welcome Mark Manion, David Stern and Bruce Umbaugh on board as our new Committee Members starting July of this year. And a special welcome to Marvin Croy as our new Committee Chair.

Computing and Philosophy conferences in the US are now meeting alternately at OSU and CMU during August. The 2003 CAP will be held on August 7, 8, and 9 on the Oregon State University campus in Corvallis. Go to http://oregonstate.edu/groups/cap for more information (BTW, www.iacap.org is the general resource for these kinds of events).

It is really incredible how much is happening these days in this area of our profession. We should all be very proud of these accomplishments and excited about what the future holds!

EVENT HANDLERS

Conversation with Pat Suppes

Marvin Croy
University of North Carolina, Charlotte
mjcroy@email.uncc.edu

When I met Pat Suppes for this interview, I had not seen him since 1978 when, as a graduate student at Florida State University, I was part of a team investigating the possibilities of transporting the Stanford logic program. After 24 years, I found Pat to be much unchanged and, true to my memories, a man of conviction, vigor, and relentless optimism. His accomplishments foreshadow the empirical trends in contemporary philosophies of mind and science. This interview took place in Pittsburgh, August 2002, during the CAP conference where Pat was awarded the Barwise Prize in Philosophy.

Croy: Philosophers interested in computers probably associate the name of Pat Suppes with the Stanford Logic Program, but your early CAI work was actually with children in elementary schools. How did that get started?

Suppes: Well, I came to Stanford after taking my Ph.D. at Columbia in 1950. I was interested in Set Theoretic approaches to a variety of problems in the philosophy of science and mathematics. But in respect to education and children, it was in 1956 that my oldest child, Patricia entered the first grade. I had a colleague in math who also had a daughter starting school at that time, and we were both frustrated at how little learning seemed to be occurring in the first grade. That got me thinking about learning and the possibilities of new educational approaches. I eventually wrote a book introducing set theory at the elementary school level.

Croy: So, how did the idea of using computers arise?

Suppes: January 1963 was an important date in that respect. I was working with Bill Estes on learning theory, and in the Fall of 1962, Dick Atkinson and I had made a proposal to the Carnegie Corporation for building an automated learning laboratory. In January, 1963, John Gardner, then head of Carnegie, called Wallace Sterling, then president of Stanford and said "I'm going to give these guys a million dollars." That was a lot of money in those days. So, we got funded and began setting up a computer-based learning laboratory. We used a computer for the automatic presentation of stimuli to subjects. This suggested to me a question: "why not use computers to automatically deliver instruction to students?" I've explored this question in various forms for many years.

Croy: And this led to your use of CAI in elementary schools?

Suppes: Yes, eventually. In our learning lab, Dick focused on reading and I focused on math. But we didn’t have enough student subjects for our experiments, and we couldn’t bring them all to Stanford, so we went out to the schools. Eventually, this led to more efforts in using computers to teach. In 1964 we were awarded a contract by the U.S. Office of Education. Our objective was to develop and assess computer-assisted tutorials for teaching mathematics and reading in the elementary schools. Obviously, in the days of massive computers, the computing power had to be at Stanford, so we connected the elementary schools via phone lines, multiplexers, and teletypes to the computer at Stanford. The teletypes were reliable but they were devilishly noisy, so they usually ended up in the supply closet in the back of the classroom. Students would file in and out of those closets all day long to use the teletypes. The logic tutorial was designed to be a stand-alone introduction to symbolic, sentential proofs. Help was available via an attendant in the terminal room, and some students benefited from this, but no group instruction or interaction was provided.

Croy: So there was enough computing power in the 60's for these efforts?

Suppes: Yes but you have to remember that these were the days when 'computer' usually meant some person operating a calculating machine for cranking out statistics like regression analysis. When the IBM 605 appeared, this was a big step forward, since it allowed many calculations to be carried out automatically. But we just made good use of the computer technology available and grew with it over the decades.

Croy: And what was the result of those efforts?

Suppes: We discovered that children can learn logic and even proof construction at an early age. The simple syntax of sentential logic encourages this, and proof construction is much easier than, for example, dividing by fractions. The emphasis on proof construction put us in a position to use the computer for more than just drill and practice or multiple-choice. We worked with a wide variety of students in several different states nationwide, including deaf students. Deaf students are interesting because, even if they can sign well, they can still have trouble with written language. Deaf student teachers are some of the best teachers in public education, and we found that, much like other students, deaf students could learn logic.

Croy: So when did CAI for logic get started at Stanford?

Suppes: I first offered logic as a complete computer-based course at Stanford in the Spring of 1973. In that course, I was only the master of ceremonies, and there were no scheduled class meetings. However, teaching assistants were available...
to answer questions, but the assistants answered questions about course administration and program functions as often as they did about the logical subject matter, so the program was doing most of the teaching. Now, when students are given complete freedom in this way, problems can arise. And at Stanford, faculty are frequently amazed at the ability of their students to concoct the most wonderful explanations (i.e., excuses) for why a task could not be completed. So, we did find it necessary to implement check points at certain junctures in the course so that students who hadn’t completed a certain amount of work were notified and eventually dropped. This course has been highly successful and continues in operation to this day. And in 1974, I introduced a computer-based course in axiomatic set theory. Nevertheless, developing good instructional software is surprisingly painful. It requires lots of data gathering and analysis to keep its multidimensional endeavors focused and on track. I’ve always been infatuated with data and with analyses that illuminate a subject.

Croy: So you found that the computer could take over the task of teaching?

Suppes: Yes, I ran the radical experiment in determining whether you could turn teaching over to the computer. We showed that it was possible, that it could be done under the right conditions. In fact, it’s been so successful that for years I’ve been able to point out to university administrators (at the appropriate moment, of course) that I carry the largest teaching course load of any faculty member at Stanford, at least 9 courses per year. In particular, computer-based courses can be useful for providing important courses whose enrollment is nonetheless too small to support adequate offerings.

Croy: Say something about your more recent projects.

Suppes: I’m currently working with Stanford’s Educational Program for Gifted Youth (EPGY). We develop courses that are available to gifted students across the nation at all levels of instruction, from elementary school through college. By taking these courses, students can earn credit in Stanford’s Continuing Studies Program, and this credit often transfers to their own schools or to colleges when they pursue higher education.

In another project, I’m working with Title I schools, those schools which have students of low aptitude and usually low socioeconomic status. We can identify talented students even within this population and we’re working to help them as much as possible.

Croy: In 1970, long before microcomputers or the internet, you predicted the rise of computers both in schools and in homes. What do you now expect for the future?

Suppes: There are three factors which I expect will favorably affect the use of computers for education. First is the growing trend toward life-long learning and continuing education. Second is the existence of alternative schools and home-schooling, and third is the general technology-driven change in patterns of work and study. Certainly, schools will not be completely replaced by computer technology, but increasingly education will take place in the home or at the work place, or as the gurus say, “anyplace, anytime.” Education at all levels will have to adjust.

Croy: You’ve accomplished and published an enormous amount. Any insight into what drives that?

Suppes: Whenever I start thinking about something, I write about it. Certainly, I’ve been at the right place at the right time, and I’ve followed where my intellectual interests and the times have led. Developments in computers have led and continue to lead in what are perhaps the most intriguing directions of our day. I’ve learned a lot from both my colleagues and my students, and that’s been gratifying. Incidentally, many of those I taught and worked with have spent time at Carnegie Mellon, where this CAP conference is being held, people like Preston Covy, Dana Scott, and Wilfried Sieg. In sum, I’ve been very fortunate to have been surrounded by talented, motivated colleagues.

In the early days of developing CAI, we were interested in the big picture and all parts of it. We knew that progress had to be made in many directions (instructional design, speech production, student modeling, theorem proving, etc.) yet we never hung back. We often invented what we needed. We once even ran our own communication line to a nearby school when the telephone company dragged its feet. It’s probably still up there! There are lots of problems in the world and one just tackles those that seem best suited for one’s talents. The past has been exciting and the future is no less so.

---

WEBSITE SEARCH

The Radical Academy: Philosophy, Politics, and the Human Condition

Kenneth Einar Himma
University of Washington
himma@u.washington.edu
http://faculty.washington.edu/himma

The Radical Academy website (http://www.radicalacademy.com) seeks to promote discussion on “traditional philosophical, moral, and religious questions; contemporary political, social, and cultural problems and policies; current scientific and technological issues and speculations; challenges to the ‘conventional’ wisdom, ‘popular’ ideologies, and ‘accepted’ paradigms of our culture; and the application of common sense realistic principles to all human affairs.” It is maintained by The Center for Applied Philosophy, which bills itself as “a Think-Tank in Cyberspace.”

The site contains a number of different features: a collection of writings by Mortimer Adler; a collection of writings by Jonathan Dolhenty; a section devoted to describing the history of philosophy; a section devoted to critiques of various philosophical positions; a section devoted to explaining the views of “the classic philosophers”; resource centers for philosophy, religion, and politics; a collection of philosophical quotations; a glossary of philosophical terms; and a forum and chat-room for discussing the various thinkers and ideas. The layout of the site is fairly straightforward and functional: primarily text-based with little in the way of graphics.

Much of the content is partisan – though not in the sense that one would expect given the prominent place of the term “radical.” The site defines “radical” (and hence itself) as “going to the foundation or root of something; fundamental; basic; getting to the basic facts, causes, principles, problems, solutions; also describes a person advocating such.” The Academy sees Aristotle as being emblematic of the sort of radicalism they wish to espouse: “an advocate within the commonsense philosophical tradition of Classical Realism.”

Jonathan Dolhenty describes the realist approach as presupposing that “philosophy is a genuine science in its own right, a systemized order of true knowledge, and that its principles and judgments are based on objective evidence
open to any observer.” The Radical Academy’s realism is, on his view, firmly grounded in what common sense discloses about the world – though Dolhenty acknowledges that common sense is reliable only to the extent that it is subjected to objective examination against rigorous standards of evidence and logic.

Not surprisingly, then, pieces tend to defend positions that are far from being “radical” in the usual sense that connotes a challenge to the conventional common sense of the day. The site contains pieces defending the following philosophical positions: moral principles are objectively true; human beings freely choose their behavior; and human beings have certain natural rights in virtue of being persons that must be respected by the state. It dismisses idealism, materialism, scientism, determinism, moral relativism, and epistemological skepticism as “false and, therefore, nonsense.” Apart perhaps from the idea that falsehood implies nonsensicality, these are not positions that one would normally characterize as “radical.”

Regardless of whether one shares the Radical Academy’s point of view, the site contains much that is interesting, helpful, and informative. There are, for example, timelines devoted to philosophy and American philosophy that list various influential thinkers along with years of birth and death. There are diagrams that depict the relationships between prominent schools of thought and diagrams that explain the various subdisciplines in philosophy. The three resource centers provide fairly comprehensive and well-organized catalogues of websites devoted to philosophy, religion, and politics.

The site also features a good bit of substantive philosophical content. Many of the articles, for example, attempt to provide an accessible but comprehensive survey of various schools of thought, philosophers, and trends. The article on Aristotle is representative of what the site attempts to provide in the way of content. The essay is divided into the following sections: I. The Life of Aristotle; II. The Works of Aristotle; III. Introduction to Aristotle’s Doctrines; IV. Theory of Knowledge; V. General Metaphysics; VI. Cosmology; VII. Psychology; VIII. Ethics; IX. Politics; X. Religion and Art; XI. Deficiencies of Aristotle’s System; XII. Aristotelianism. There are similar articles devoted to thirty-eight philosophers who span the Ancient, Medieval, Renaissance, Modern, and Recent Periods.

Unfortunately, this content is often unreliable. One essay, for example, blames Descartes for the lay popularity of the claim that truth is subjective: “Descartes (1596-1650) is the philosopher most noted for the beginning of the philosophic disaster which was to come. He sharply separated reason from the senses and, being distrustful of sense knowledge, declared that only through our clear and distinct ideas could we have valid knowledge. Ideas were not based on sense knowledge, but were innate in the mind and could be brought to consciousness and developed into knowledge without the aid of experience. This and many other nonrealistic principles were introduced by Descartes into modern thought.” Among other problems, this overlooks the fact that the very point of Descartes’ famous Meditations was to put sense knowledge on a firm epistemological foundation. Though there is undeniably some useful and interesting content on the site, the reader looking for general philosophical information is more likely to find reliable content by visiting the two online philosophy encyclopedias: Stanford Encyclopedia of Philosophy (http://plato.stanford.edu) and Internet Encyclopedia of Philosophy (http://www.utm.edu/research/iep).

More useful, depending on one’s political tastes, is an online newsletter that is largely devoted to political articles. Not surprisingly, the articles generally reflect the Radical Academy’s “authentic libertarian [commitment] to . . . a free-market economy without unnecessary government interference and . . . a limited government under a constitutional covenant.” Recent offerings include essays entitled “This is Justice? Gun Control Out of Control”; “Another Libertarian Wins Nobel Prize”; “Esquire Survey: Reagan Greatest American, Clinton ‘Most Loathsome’”; and “Major U.S. Religious Body Calls for End to Drug War.”

There is some advertising on the site but it is, relatively speaking, fairly inconspicuous. Most of the advertising is reserved for specific Academy pages that seek to support the site with sales of books and magazines. Most of the advertisements are for booksellers such as Amazon.com, Powell’s Bookstores, and Alibris Books (the Radical Academy asks visitors to support the site by buying from its bookstore). If the increasingly commercial character of the web is taken as the standard, what advertising there is seems unobjectionable.

On the whole, the site is something of a mixed bag. Because it tends to offer a one-sided (and sometimes unreliable) perspective on various philosophers and philosophies, it is not as useful as some of the other general philosophy sites that have been reviewed within these pages. Even so, the political content is frequently interesting and provocative and the various resource centers do a nice job of supplementing some of the other philosophy portals. It is certainly worth at least one look.

---

**Computing Ethics**

**Endgame: Ethics and Values in America and Morality and Machines**

Douglas Birsch  
*Shippensburg University*  
drbirsch@ship.edu

“Endgame: Ethics and Values in America,” is an extremely interesting website and Stacy Edgar’s computer ethics textbook, *Morality and Machines* is worth investigating. The Endgame website was created by Scott Goldstein and produced by Vulcan Productions for PBS (http://www.pbs.org/endgame). This website can be used in connection with any ethics course, including a computer ethics class. It provides a variety of materials to explore an ethically significant case or scenario. The site features nine main parts: two videos, three questionnaires, a question-and–answer session with the key characters, a selection of opinions from some “ethical experts,” and two summaries of the results of the questionnaires.

The first part is a video that presents an ethically significant event and several important decisions related to it. Two women, Julia and Alison, are driving on a lonely road and Julia causes an accident that kills a man. Julia has been responsible for establishing an educational foundation that has helped many young people. She is driving home from a banquet honoring her and marking the occasion of the foundation’s being funded to provide national assistance. Julia has had a couple of drinks and Alison suggests that she wait until talking to a lawyer before reporting the accident to the police. Julia
initially accepts this suggestion, but never calls the lawyer and decides not to report the accident because of the possible adverse effects on the foundation. She also pressures Alison to refrain from reporting the accident. A survey following the video contains five questions related to the viewer’s opinion on whether Julia and Alison are doing the “right thing” and on what the viewer would do in the situation. This first survey is followed by a second video showing Julia and Alison’s subsequent conversations about the incident. Neither one of them informs the police. The authorities discover that the victim’s blood alcohol level was above the legal limit, so the police regard that as the cause of the accident. It appears that Julia’s role in the tragedy will remain undetected, but her relationship with Alison has become strained. A second survey, containing the same questions as the first one, follows the second video. Presumably the viewer is being given the chance to change his or her mind about the answers.

Next, there is a question-and-answer session with the two people from the videos: Julia and Alison. The questions are stated in writing and the answers are provided by short videos featuring the women. Following the question-and-answer session with the women, there is a selection of opinions from three real-life “ethical experts.” The first one, Michael Josephson, is the founder of the Joseph and Edna Josephson Institute of Ethics and the Character Counts Coalition. David Kaczynski, the second “expert,” turned in his brother Ted Kaczynski, the Unabomber, to the FBI. Having made this extremely difficult decision, he has some first-hand knowledge of ethical dilemmas. Finally, Jackie Joyner Kersee is an excellent athlete who has been very active in helping charities. Her extensive charitable work, not her athletic ability, presumably qualifies her as an “ethical expert.” This session is followed by a final questionnaire containing the same questions as the previous ones.

Next, there is a survey that shows the viewer’s answers to the questionnaires. This allows the viewer to see at a glance whether he or she has changed any of the answers. The last component of the site is a chart of the results of all the viewers’ answers. This allows the viewer to compare his or her answers to those of others who have participated in the website. Thus, the site contains a fairly extensive ethical exploration of the scenario related to the automobile accident.

The Endgame website is an interesting tool for use in an ethics class. It is not about a computer ethics issue, but it clearly illustrates one ethical dilemma and shows how reasonable people can disagree about how to resolve it. Thus, one way to use the site would be, at the beginning of the course, to give students an initial example of an ethical dilemma and disagreement over its solution. Alison seems to think that the “right thing” for Julia to do is to tell the truth. She talks about the right of people to know the truth and respect for the law and other persons. She represents a deontological view of morality. Julia, in contrast, hides the truth in order to bring about the greatest benefit for the greatest number of persons, the thousands of students who will be helped by her foundation. She appears to believe that she is essential for the foundation’s success and that a scandal involving her would destroy the foundation. For her, the truth must be sacrificed for the greater good of the majority of persons. She represents a consequentialist or act utilitarian position. Thus, the case illustrates two different ways of resolving ethical dilemmas.

The site could be used during a course to introduce deontological and consequentialist/utilitarian approaches to morality. It might also be used after discussing these approaches to illustrate them. I found the question-and-answer session with the women more interesting and more appropriate for use with students than the opinions of the “ethical experts.” The experts’ comments are not preceded by questions and this makes it harder to quickly appreciate their focus and relevance. Also, the women’s comments need no explanation, but some of the remarks made by the experts need some clarification. It would be interesting to ask students to play the role of an “ethical expert” and see if they could do it in a clearer and more useful manner. Students could also role-play Julia and Alison to get a better feeling for the situation. The videos are excellent, clear, and extensive enough to adequately set up the scenario. The idea of asking the viewers questions and having them commit themselves to answers is valuable. It makes the site interactive, instead of merely passive. In a classroom, the instructor would presumably ask students to support their responses with reasons. The chart showing all the viewers’ answers is also a worthy inclusion. I was surprised by the results. Of course, there is always the question in regard to such polls as to whether people provide a truthful answer or instead try to give the answer that they think they are supposed to give. One other way of using the site would be to see it as an interesting model that students could be asked to emulate using computer ethics cases. A group of computer science majors should have the knowledge to replicate most of the site with a different case.

Moral philosophers, interested in computer ethics, are involved with applying ethical concepts and theories to issues related to computer technology. Some of them are also interested in the effects of computers on ethics and ethical issues. Does presenting this moral issue using computer technology have any effect on the issue? One effect is that the presentation using computer technology makes the issue more interesting to most people. The website is visually attractive and easy to navigate. It grabs the viewer’s attention in a way that a book probably would not. The videos present the problem in a more appealing way than a written summary of the case. The question-and-answer session with the characters is also more interesting than a transcript in a book. Another effect of using computer technology is that the issue probably has a greater impact on the viewer. The video powerfully illustrates that ethical problems can arise for anyone. The videos also forcefully show the impact of the problem on the women. The website makes the ethical problem or issue affect most viewers more strongly than a written treatment would.

The presentation on the website has a couple of potential negative effects, but these seem to be related more to content than the computer technology. First, the presentation seems to obscure morality, at least on Alison’s side. Alison and the experts talk about “doing the right thing,” but do not explain why it is the right thing to do. There is no justification, for example in terms of a Kantian morality, for “telling the truth” being the “right thing to do.” Alison and a couple of the “ethical experts” seem to think the “right thing” is obvious, but this obscures the morality that makes it the right thing to do. The computer technology may tend to lead people to take a quick look at problems or issues, but it does not have to do so. If the producers of the site wanted to keep the site relatively limited, they might have provided hypertext links to other sites with more philosophical content. In contrast, they might also have provided an additional page or pages that made explicit the connections between the women’s respective positions and utilitarian and Kantian morality.

A second potential negative effect is that the voting in the surveys and the posting of the results of all the viewers’ votes may give some people the wrong impression. In democratic
Politics, the majority wins. It should be made clear that the ethical “right thing to do” is not created by a vote of the majority. The voting is presumably designed to make the site interactive by involving the viewer and has no connection with the morality that informs the moral evaluations. When using a computer or any other technology, it is always important to pay attention to the messages that the technology may convey. The computer technology that allows the voting may send the message that the opinion of the majority creates the “right thing to do” as well as making the site interactive. On the whole, however, I think that the computer technology has a positive effect on the viewer by making the issue and ethics more interesting and forceful.

At 522 pages, Morality and Machines by Stacey L. Edgar is the most extensive computer ethics textbook that I have encountered. In contrast, Deborah Johnson’s popular Computer Ethics is 240 pages. Edgar’s book, published in 2003 by Jones and Bartlett Publishers, is in its second edition. The purpose of this textbook is to make the readers aware of the moral problems related to computers and to provide them with the knowledge necessary to identify viable solutions to them. Readers will learn about the possibilities for computers to improve their lives and also about the dangers associated with them. The volume contains twelve chapters and three appendices. The first two chapters explore several views that challenge the possibility of ethics or morality, and provide arguments against them. Chapter 3 examines some basic ethical theories. Chapters 4 through 12 explore issues related to computers and information technology. Chapter 4 concerns software privacy and the issue of property and its protection. Chapter 5 looks at computer crime. Unauthorized access, computer viruses, and computer worms are among the topics discussed in Chapter 6. Chapter 7 is titled “Privacy,” while Chapter 8 is “Errors and Reliability.” Computers and the workplace is the subject for Chapter 9. Chapter 10 involves issues related to responsibility, liability, law, and professional ethics. “Computers, the Government, and the Military” is the title of the eleventh chapter. The final chapter is about artificial intelligence and virtual reality. Each chapter is supplemented by short and long essay questions, references, and recommended readings. The chapters are well written and should be accessible to a wide range of students. They contain sufficient information to understand the issues and a wide range of examples. The lists of recommended readings are very impressive and provide a summary of the most significant works on each issue. Three appendices, the first of which provides topics for term papers, follow the chapters. The second appendix contains the ACM Code of Ethics while the third one includes the IEEE Code of Ethics. A bibliography and an index follow the appendices. Morality and Machines is an impressive and extensive textbook that displays a great deal of thought and research. For an instructor looking for a comprehensive monograph with a short introduction to ethical theories and a wide range of issues related to computer technology, it would be well worth investigating.

I hope you find this information useful. Please feel free to send me reviews of scholarly books, textbooks, journals, or websites (dbirs@ship.edu). I am also interested in short articles on any topic related to computer ethics and information technology.

### Teaching in Cyberspace

**LogicWorks: The Next Generation**

Rob Brady, program author
Stetson University
rbrady@stetson.edu

LogicWorks: The Next Generation is an interactive, multimedia logic course delivered to students on a CD-ROM. It includes all of the content, exercises, examinations and (eventually) supplementary readings normally used in a college level introduction to logic course. In addition, it provides the student with interactive exercises and practice examinations, includes materials for use in classroom lectures, administers examinations, grades the students’ work, and maintains a grade book for the instructor. Communication outside the classroom between students and instructor is made simple via the Internet.

The new LogicWorks creates the learning and teaching environment of the 21st century. The students’ learning environment is enriched by the interactivity, by the full integration of multimedia, and by easy access to the instructor and the necessary course materials. The professor’s teaching environment is enriched by the focus on the students rather than on assembly of course materials and grading.

The program was published in December of 2003 by the Philosopher’s Information Center, a non-profit research institute. This new program is a successor to work that I have been involved in for almost 20 years. In 1986 the first program, The LogicWorks, was published and eventually went through 8 editions and was used at over 200 universities. That program appeared at a time when few logic courses used any software. Among the features of the program designed for students are the following:

1) A complete introductory logic text is included and can be read from within the program or printed;

2) Normal things one would do with a text—highlighting, book marking, and writing marginal notes—are readily available and intuitive;

3) Over 750 exercises, ranging from critical reasoning problems to predicate logic, are interactively graded with hints given when mistakes are made;
4) Practice examinations are available and can be modified at the instructor’s discretion;
5) The program tells the student when assignments are due and shows the homework score by chapter and overall;
6) The student can turn in homework (already graded, of course) to the instructor via the Internet;
7) When taking an examination, the student can review each answer and change it if desired, prior to turning in the exam and receiving the results;
8) After taking an examination, the student and the instructor can review exactly what the student entered and, if needed, can even rework the problems to find the correct answer;
9) Study guides for each chapter are included and can be printed by the student for reference;
10) The text will read itself to the student, turning pages as it goes (this feature is especially useful for students with disabilities);
11) The program allows a choice of symbolic fonts and the chosen font will appear consistently throughout the text and the exercises;
12) Numerous help screens are available throughout;
13) The program operates independently of the Internet and consequently can be used by students who do not have Internet access;
14) Each student has a personal ID number which provides access to the program and insures that the student receives credit for work done;
15) Updates of the syllabus, the assignments, the program, the text, etc. are quickly available via the Internet.

Among the features of the program designed for instructors are the following:
1) All grading is done by the program, though the instructor may choose to give additional work and enter the grades in the program’s grade book;
2) All record keeping is done by the program;
3) Multiple sections are easily managed;
4) With the proper classroom setup, the entire text can be used as a classroom aid;
5) Actual examinations can be given with LogicWorks and are automatically scored and entered into the instructor’s grade book;
6) Assignments and course syllabi can be set by the instructor and distributed via the Internet;
7) Actual examinations are constructed easily by selecting exercises already in the text, and new problems can be added by the instructor;
8) The examinations, once created, can be quickly and easily tested (the program will even enter most of the answers for you);
9) Paper examinations can be created automatically from the electronic ones and can then be further edited;
10) Examinations and other materials are encrypted and can only be read from within the program;
11) Passwords set by the instructor control the taking of examinations and the posting of homework;
12) The text, including the exercises and the answers, can be printed;
13) While working with the program the instructor can have the correct answer displayed (proofs, Venn diagrams and truth tables are exceptions);
14) The instructor can edit the text and edit the responses to the exercises;
15) From within the program the instructor can read or print the instructor’s manual;
16) A detailed report on each student’s work shows which problems have been worked, how many times they were tried, and what the final score was;
17) A class summary is available which allows the instructor to easily adjust grades for individuals or for the entire class (the changes can be posted back to the students’ personal computers);
18) The students’ grades are determined by the assignments, by the weighting of the homework, and by the weighting of the examinations set by the instructor;
19) The instructor can select the logical symbols to conform to any subsequent courses;
20) The study guides can be expanded or modified by the instructor, and other class materials can be distributed via the Internet;
21) The program can be installed on a local server for proctored examinations or for lab use by students who have a valid personal ID.

Despite the many things which the program already does, I regard it as more of a beginning to my overall project. My goal is to create a fully adaptive multimedia learning and teaching environment. Though the program currently begins with an interview of the student, asking for the student’s
In this paper, we demonstrate how, with the support of an Ethics Across the Curriculum (EAC) initiative, academic programs in computer science and technology in the undergraduate curriculum can successfully integrate ethics. More specifically, we will describe how the EAC program at Saint Louis University helped the computer science units:

- Fund the development of the new course and course modules;
- Obtain approval of the new course and course modules;
- Address the issue of who is qualified to teach the courses;
- Design course activities and assignments to meet the goals of the course;
- Foster new opportunities through program growth and development.

Ethics Across the Curriculum at Saint Louis University

The Ethics Across the Curriculum Program at Saint Louis University was created in 1998 by faculty, for faculty. It is an interdisciplinary faculty development program that aims to address the challenge of how to improve the moral education of our students. The program rests on the belief that the purpose of a university education, especially a Catholic, Jesuit one, is not simply to provide students with the tools and skills necessary to earn a good living, but also to lead a good (moral) life. The development of a process of moral reasoning is critical to this task. Students must learn to think critically and knowledgeably about ethical issues. This is a task that cannot be completed in a one-semester course in ethics (something required of all of our students) but rather is something that must be reinforced via a systematic application of ethics across the curriculum.

In response to this challenge, the EAC Program aims to inspire, enhance, and sustain teaching, research and service as it relates to ethics at the undergraduate, graduate and professional levels. Program goals include:

- Identifying efforts across the University that focus on ethics;
- Facilitating exchange of information and resources among academic units;
- Sponsoring lectures and workshops to stimulate conversations about ethics;
- Providing developmental opportunities for faculty to become more informed about descriptive and normative ethics;
- Offering a supportive environment in which faculty can explore the ethical issues relative to the classes, laboratories, and other settings in which they teach and develop curricular materials that focus on these issues; and
- Building and sustaining a moral community of discourse among the faculty, i.e., fostering a university-wide commitment to the ethical mission of Saint Louis University in faculty research and teaching.

In the pursuit of these goals, the program has implemented several initiatives on campus, always with a focus on faculty development. Two significant initiatives have contributed to the integration of ethics into the computer science curriculum: the summer workshop for faculty and the Summer Stipend Award Program.

Each summer since its inception, the EAC program has sponsored an annual summer workshop for faculty.
objective of the workshop is to offer a foundation in both philosophical and theological traditions in ethics, as well as a brief overview of some contemporary critiques. The sessions provide a common ground of discourse as a community of scholars as well as a general understanding of the material provided to university students in their required theological and philosophical ethics courses. In addition to providing the theoretical foundations, the workshop also provides an opportunity to address the application of these approaches as well as explore pedagogical techniques for addressing ethical issues in the classroom.

The program also administers a Summer Stipend Award Program. This is a competitive award, and proposals must demonstrate exceptional merit and value for the individual, the department, and the mission of the EAC program. Stipends of $2,500 are available for research activities, course and curriculum development, and/or faculty development that provides for the integration of ethics with the applicant’s discipline. As a requirement of receiving the award, each recipient submits a final report to the program on the accomplishments of his/her project and attends a roundtable meeting in the fall to discuss their projects and accomplishments with interested faculty.

**Development of a Dedicated Course on Computing and Society**

At Saint Louis University, the Department of Computer Science is housed in the Parks College of Engineering and Aviation. The College requires all of its students to complete a set of courses comprising a core curriculum. Included in this core are courses in Philosophy, Ethics, Theology, Cultural Diversity, Psychology, and other courses in the social sciences and humanities. Students seem to view the core curriculum as a set of “required courses” for graduation. Moreover, they have very little opportunity to understand the significance of the “well-rounded educational experience” they are offered at Saint Louis University while they are in college. Thus, in order to help students appreciate the natural connection that exists between the “technical” major they are pursuing, and the “non-technical” subjects they are required to take, the Department of Computer Science developed an ongoing dialogue with the Philosophy Department and the EAC program.

Moreover, while requiring the student to obtain exposure to the so-called “non-technical” fields, the Computing Sciences Accreditation Council (CSAC) of the Computer Science Accreditation Board (CSAB), has recently developed a new set of standards for Computer Science programs that include treatment of ethical and social aspects of computing in the undergraduate Computer Science curriculum. Thus, the Department of Computer Science decided to pursue the dialogue in the direction of developing a “Computing and Society” course for the undergraduate Computer Science major.

Discussion of ethical issues arises in the very first course in Computer Science when information privacy and protection of intellectual property are emphasized through user-id and password requirements for access to computing facilities at the University. However, the vast amount of technical material that needs to be covered in this course almost forces the instructor only to mention casually the significance of information protection and privacy matters. Beginning students tend to view computer programs as mathematical problems that are routinely solved in the classroom, without understanding that copying or cheating on a computer program can be categorized as plagiarism. Thus, the authors feel that it is necessary to provide opportunities for the Computer Science major to be involved in discussions related to these matters via a dedicated course on the social and ethical aspects of computing.

It did not take much time for the Department of Computer Science to realize that offering “Computing and Society” as a course independently taught by a Computer Science instructor posed big challenges. The instructors needed to educate themselves in the philosophical traditional in ethics as well as strengthen their skills in critical thinking and logic. This is what prompted the participating authors of this paper to attend the summer EAC workshop, and pursue the Summer Stipend Award for the development of courses to integrate ethics in the Computer Science curriculum.

Computer science educators typically have little formal background in philosophy and ethical debate. This was certainly the case on our campus. Thus, these instructors often feel underprepared to develop and present modules or courses addressing ethical issues. The workshop presented by EAC provided some foundational resources for the interested instructors. In addition, EAC provided support to the instructors with regard to curriculum development, including lectures, assignments, grading, etc., as well as acting as “team-teacher” for the initial offering of the course(s) and/or modules.

One of the accreditation issues is the so-called “bean counting,” which is the ordeal of making sure that a certain number of credit hours have been allocated in the technical curriculum for certain key areas within the technical subject matter and related disciplines. These programs somehow manage to include the least number of credit hours required for the seemingly unrelated non-technical subjects. Thus, getting a dedicated course on Computing and Society approved through the curriculum committees and other faculty governance structures within the College of Engineering posed a challenge as well. Two important measures helped us in this regard. First, a six-hour Philosophy requirement for the Computer Science majors was replaced with 3 hours of Philosophy and 3 hours of the dedicated Computing and Society course. Secondly, other engineering departments within the College were encouraged to have their majors take the Computing and Society course in place of the Engineering Ethics course. It was also emphasized that the Computing and Society course would be team-taught by Computer Science and Philosophy instructors. The EAC program, the Philosophy Department, and the Department of Computer Science were actively involved in the dialogues leading to the approval of this course at the College Faculty Assembly level.

Given a choice, a Computer Science instructor would prefer to teach a programming course instead of a Computing and Society course. Even after attending an EAC workshop, faculty members need not feel fully prepared to teach such a course. However, at Saint Louis University, the interaction between the Department of Computer Science and the School for Professional Studies offered a naturally viable solution to this dilemma. The Director of the Computer Science Technology degree program at the School for Professional Studies teaches a course each year for the College of Engineering. His background in the industry, his personal interest in integrating ethics in the Computer Science Technology curriculum, the nurturing-mentoring relationship that exists between the two units, and the close relationship of these two units with the EAC program all led to the successful teaching of this course in the spring 2001 semester. The Director of the EAC program was available to provide discussion of ethical theories that facilitated the discussion of ethically contextual case studies in Computer Science. Guest
speakers from the industry and from the Saint Louis University Office of Information Technology Services reinforced the need to study the ethical issues in computing in a formal setting.

In the following, we briefly describe the Computing and Society course as it was taught for the first time at Saint Louis University. Three main aspects of the course will be described: the learning objectives, course topics, and the student projects.

**Learning Objectives:**
The learning objectives of the Computing and Society course were developed using the 1991/2001 Association for Computing Machinery (ACM) guidelines for Computer Science curricula. These objectives were focused more on students in applied social and professional ethics rather than in theoretical ethics. They were:

- To understand the basic cultural, social, legal, and ethical issues inherent in the discipline of computing.
- To develop the ability to ask questions and evaluate proposed scenarios in relation to the social impact of computing and information technology.
- To interpret and be aware of the basic legal issues surrounding the development and use of computer software and hardware.
- To appreciate the philosophical theories that provide the framework for ethical decision-making.

**Topics Covered:**
Specific course topics covered in the course, along with the minimum amount of time in contact hours devoted to each topic are outlined below:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Time (Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>History of computing</td>
<td>1</td>
</tr>
<tr>
<td>Social context of computing</td>
<td>3</td>
</tr>
<tr>
<td>Methods and tools of analysis</td>
<td>2</td>
</tr>
<tr>
<td>Professional and ethical responsibilities</td>
<td>3</td>
</tr>
<tr>
<td>Risks and liabilities of computer-based systems</td>
<td>2</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>3</td>
</tr>
<tr>
<td>Privacy and civil liberties</td>
<td>2</td>
</tr>
<tr>
<td>Computer crime</td>
<td>2</td>
</tr>
<tr>
<td>Economic issues in computing</td>
<td>3</td>
</tr>
<tr>
<td>Philosophical frameworks</td>
<td>6</td>
</tr>
</tbody>
</table>

**Final Project:**
Students were required to research, write, and present a culminating report as a final project in the course. Teams of two or three students each were formed for this purpose. The research topic had to be within the field of computer science or information technology and of an applied nature. Each report was formally presented in class, where students were given the opportunity to challenge the ideas and views of the presenters. A sampling of the research topics is provided below for reference:

- Anonymity on the Internet
- Computers in Education
- Privacy – Computers and the Internet
- Hackers!

**Development of Course Modules for Computer Science Technology**
The School for Professional Studies within Saint Louis University has the mission to provide work-place oriented degree programs in the evening and on the weekends to working adults. The school believes that a university education should result in something more than simply a path to earning a living. It should empower a student to be a productive contributor in the community and society as a whole. With this said, the social and professional ethics component of a student’s education is critical to the transformation of future society.

The Director of the School for Professional Studies Computer Science Technology (CST) degree program became interested in how to better incorporate ethics into the CST program after learning about the Ethics Across the Curriculum (EAC) Summer Stipend Award Program. The CST Director submitted a proposal to the EAC that outlined a plan to incorporate ethics into the learning goals of the CST program by including modularized ethics-related course activities in two upper-level CST courses. The modularized format was chosen because it provides an easy way to incorporate ethics within existing courses. The courses that were selected are CST 300 – Software Engineering and CST405 – Project Management. Both courses are required and at a junior/senior level where the students should have the foundational knowledge necessary for critical thinking and reflection. Three deliverables were identified in the EAC proposal:

- Course syllabi will be updated to include ethics-based learning objectives and concepts.
- Detailed lesson plans will be developed for classroom lectures. These lesson plans will include PowerPoint-enhanced slide shows on each topic.
- Evaluation will be used to assess students’ understanding of ethics in Computer Science Technology. This will include formal quizzes/tests, group discussions, case study evaluations and/or reflective journaling.

Most courses within the School for Professional Studies are taught by affiliate part-time faculty. This presented a special challenge for incorporating ethics into the CST program. All the background information and course activities would have to be developed in a way that could be easily conveyed to affiliate faculty. The EAC program provided guidance in selecting course topics and activities and in modularizing the class materials.

The learning goals for the modules were developed with an emphasis toward student outcomes in applied social and professional ethics, rather than in theoretical ethics. The learning goal for the CST300 – Software Engineering course is to develop skills to reflect on computer science-related ethical dilemmas in the workplace. The learning goal for the CST405 – Project Management course is to develop an understanding of and appreciation for professional codes of ethics. Specific topics covered in each course are listed below:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized use of computers</td>
<td>CST300</td>
</tr>
<tr>
<td>Hardware, software, and information theft</td>
<td>CST300</td>
</tr>
<tr>
<td>Information privacy, copyright, and objectionable materials on the Internet</td>
<td>CST300</td>
</tr>
<tr>
<td>Ethical reflection – standards and norms used in business</td>
<td>CST405</td>
</tr>
<tr>
<td>Professional ethics (codes of conduct)</td>
<td>CST405</td>
</tr>
</tbody>
</table>

The EAC program provided suggestions and guidance in evaluating specific activities that were used to reinforce ethical concepts. The computer science faculty provided professional expertise so that the scenarios were reflective of real-life scenarios in the computer science profession. Several classroom activities were developed to encourage the students to reflect upon basic ethical decision-making. These activities illustrate ways to incorporate basic ethical decision-making...
into real-world computer science applications. Two examples are listed below: the worksheet and the position paper activity.

**Worksheet Activity**

The worksheet activity is a good icebreaker and requires very little preparation from the students. The purpose of the activity is to introduce the sorts of ethical issues that will be addressed in the course and to help students get comfortable with class discussion. Students are handed a one-page worksheet that lists computer-related scenarios and are asked to individually rank each statement as being ethical, unethical, or a crime. Once the students have completed the worksheet, the instructor tallies on the chalkboard the results for each question. The instructor initiates discussion of the questions by calling upon students and asking them to explain their choice. Listed below is a sample worksheet.

**Worksheet – Ethical/Unethical/Crime**

This activity is derived from an exercise in *Teachers Discovering Computers* (Shelly, Cashman, Gunter, and Gunter, 1999.)

The purpose of a position paper is for the students to develop and present reasoned opinions on matters of ethical relevance. The students are presented with a simple scenario in the form of a case and asked to identify the central themes. Then the students are asked to determine if the actions taken can be ethically justified or not. Students research the topic and look for related cases or situations that are similar in real life. Listed below is a sample position paper.

**Position Paper – Software Reliability**

A software company just created a tax software package that incorporates new tax laws and figures for the year. The president of the company knows that the program probably has bugs in it. He knows that if his company is the first to market this product, they will capture the largest market share. He decides to release the program with a disclaimer stating that his software company is not responsible for errors resulting from or due to the software. The software company released version 1.0 to the public first and captured much of the market. However, the software caused several users to file incorrect tax returns and, subsequently receive penalties from the IRS.

What ethical issues are central to this case study? Were the actions of the president ethical or not? Is it ethical to market a product with a disclaimer releasing the maker of errors?

**New Opportunities**

As a result of the increased awareness of and emphasis on ethics, the computer science programs have undertaken additional curriculum and research initiatives including the development of a freshman seminar course, the development of a grant proposal to the National Science Foundation, and co-sponsorship of a one-day conference on Ethics in Science Education.

**Freshman Seminar Course**

The computer science department at Saint Louis University currently has a proposal in the works to introduce a new freshman seminar “Computing for the Society: The Technical, Social, and Ethical Aspects of Computing for the College Student.” This new freshman seminar course is entirely devoted to the ethical use of information technology and the impact of information technology on the society. Thus, students enrolled in this course are studying the discipline of computing from a user perspective, as opposed to the perspective of a software or hardware designer. The use of information technology, ranging from browsing the Internet to accessing public databases, will form an integral part of the course. Students will receive instruction regarding these activities in the course as well. In addition, site-visits to Data Centers will be organized so that students can learn what the real-life ethical issues in the industry are, and how they are dealt with on a day-to-day basis. The format of the course will include:

- Guest-lectures by individuals from other academic units within the University, and information technology professional from other academic institutions and from the industry;
- Classroom discussions of case studies in groups;
- Group project presentations by students; and
- Site visits to Data Centers.

**National Science Foundation**

The Computer Science department, the Ethics Across the Curriculum organization, and the Emerson Center for Business Ethics has partnered to submit a grant proposal to the National Science Foundation - Societal Dimensions of Engineering, Science and Technology division entitled “Computer Ethics – Teaching Ethics via Cases (CE-TEC).” The basic concept of the grant is that it is our belief that a science or technology based university education should result in something more than simply a path to earning a living. The university education should empower a student to be a productive contributor in the community and society as a whole. The social and
professional component of a student’s education is critical to the
transformation of future society and the environmental
landscape surrounding science and technology professions.
The proposal presents activities that would demonstrate that
through the use of applied and professionally oriented ‘case
method’ teaching strategy in the discipline of computer
science by instructors who are effective in use of the ‘case
method’ and have access to resources for teaching using
cases, future generations of professional in the IT workplace
will be better prepared to transform society using positive
ethical values.

“Ethics in the Education of Scientists, Clinicians, and
Engineers” Conference,
Dr. Asaithambi learned of a grant opportunity and initiated the
development of an interdisciplinary team to prepare and
submit a proposal to Sigma Xi: The Scientific Research Society,
to acquire funding for an “Ethics in Science” workshop. This
team, consisting of faculty representing Computer Science,
the Medical School, the Center for Health Care Ethics as well as
the Ethics Across the Curriculum Program, was successful in
gaining funding from Sigma Xi. Because of the inter-
disciplinary nature of the project, we were able to acquire
matching funding from the Graduate School, the Medical
School, and Parks College of Engineering and Aviation. As a
result, Saint Louis University hosted a one-day conference
titled “Ethics in the Education of Scientists, Clinicians, and
Engineers” on February 8, 2002.
The conference was highlighted with invited presentations by
Nicholas H. Steneck, Ph.D., Professor of History, University of
Michigan; David W. Musick, Ph.D., Vice-Chair for Education &
Director of Development for Department of Rehabilitation
Medicine & BioEthics Center, University of Pennsylvania;
James M. DuBois, Ph.D., D.Sc., Associate Professor, Saint Louis
University Center for Health Care Ethics; Michael Pritchard,
Ph.D., Professor of Philosophy & Director of the Center for the
Study of Ethics in Society, Western Michigan University; and
Muriel J. Bebeau, Ph.D., Professor of Preventive Sciences,
School of Dentistry - Center for the Study of Ethical
Development, University of Minnesota. Topics that were
discussed at the conference included: Fostering Integrity in
Research: Why, How, and the Cost?, Promoting Responsibility
in the Sciences and Professions, What Ethics Education Should
Be vs. What It Is: The Case of Medical Education, and Strategies
and Goals in Assessing Outcomes in Ethics Education.

Summary
With the rapid increases in technology today, new dilemmas
for using and applying these technologies are also increasing.
The decision makers and technology implementers of
tomorrow must have a framework from which to assess the
validity of their judgments. Developing skills in ethical
decision-making will help our students in their professional
lives and promote positive uses of technology. This paper
outlines how, with the support of an Ethics Across the
Curriculum (EAC) initiative, science-related degree programs
(i.e., computer science and technology programs) can
successfully integrate ethics into their curriculum. The two
approaches described included the development of a new
required course for computer science majors and the
development of a set of modularized mini-lessons and
activities that were incorporated into existing courses required
for Computer Science Technology students.

The authors of this paper were encouraged by the Ethics
Across the Curriculum (EAC) program to develop and expand
professional and applied ethics within the discipline of
computer science at Saint Louis University. This paper outlines
the processes and success experienced because of EAC. It is
hoped that the detailed information provided in this paper will
inspire other organizations to look seriously at developing and
nurturing similar programs within their institutions.

Endnotes
Occupational Outlook Handbook (February 26, 1999 last modified),
Online.
2. U.S. Department of Commerce, American’s New Deficit: the
Shortage of Information Technology Workers, 1999.

Platform

Power in Terror
Jon Dorbolo
Oregon State University

Francis Bacon has been in the news lately. A variation of his aphorism,
“Nam et ipsa scientia potestas est,”(knowledge is power itself)
appears on the Information Awareness Office (IAO) official seal and the IAO
has been making the front pages. The IAO develops information technology
for the War on Terror. Bacon understood that information and technology were the key to
cultural power. He identified the magnetic compass, gunpowder, and the printing press as decisive elements in the
balance of power among territories. The artifacts that he identifies equate to commerce, war, and information; the same
factors of power among nations today. The common feature
among these sources of power, says Bacon, is knowledge;
hence his claim “knowledge is power itself.”

Bacon’s contemporary, Thomas Hobbes, identifies terror as the basis of power internal to a social collective. Terror
that other people may use their liberty to harm us is what leads
us to seek a common government and to trade liberty for
security. Terror of a government’s power to punish prevents
us from harming one another. In a social contract the sovereign
“hath the use of so much power and strength conferred on
him that, by terror thereof, he is enabled to form the wills of
them all, to peace at home, and mutual aid against their
enemies abroad” (Leviathan, XVII). The terror of harm from
enemies both external and internal moves us to invest the
power to inflict harm into a central government, that it may
protect us. Hobbes’ principle can be understood as a ratio
between terror and power: the greater the terror that citizens
feel of one another, the more power the government
commands.

Hobbes depicts the most potent terror as coming from
within the society. Crime, for instance, is well known as an
effective appeal upon which politicians may build power.
During the Cold War, the fear of communism was powerfully
played in the U.S. through the image of infiltration by communism from within. The Red Scare left citizens worried
that their own neighbors, public officials, and teachers might
be the enemy. Terrorism is the 21st century replacement for
communism as a fear factor. Terrorists live among us and strike
from within. There is no telling who may belong to the terror
network. Following Hobbes, the fear of terrorism is transferable to government power. Thus, the aptly named War on Terror is primarily an internal battle with major consequences for domestic policies.

The US Government plans to fight the War on Terror with information technology;

“The key to fighting terrorism is information. Elements of the solution include gathering a much broader array of data than we do currently, discovering information from elements of the data, creating models of hypotheses, and analyzing these models in a collaborative environment to determine the most probable current or future scenario” (Information Awareness Office, 2003).

The core technology under development by the IAO is Total Information Awareness (TIA), a suite of tools for the collection, routing, and mining of data. As envisioned, TIA may be the most powerful domestic and law enforcement technology yet. If successful, it would detect patterns of criminal activity and predict terrorist attacks so that they may be prevented. Through such technologies, the IAO promises to protect us from the terror within. To gain that security, we need only relinquish some of our rights to personal privacy. We are offered a Hobbesian bargain: trade privacy for security against terror itself. As Bacon and the IAO motto scientia est potestas reminds us, that bargain confers great power to the government. In the information age, knowledge is power indeed, and total knowledge is total power.

Total Information Awareness

Perhaps more than any other publically acknowledged technology, the Total Information Awareness (TIA) project raises the specter of Big Brother (or The Beast depending on the sources of your paranoia) for many Americans. TIA is a mass-scalable data mining initiative designed to look for activity patterns in the flow of the common information stream. Email, web server logs, web search engines, telephone and cell phone records, credit card transactions, banking records, travel reservations, medical records, DNA databases, and biometric data (e.g., video camera surveillance) are among the data streams to be tapped and monitored. Just as the FBI creates psychological profiles for serial killers, TIA will use models to identify patterns of activity common to terrorist operations. What makes TIA so attractive to law enforcement, intelligence, and the military is the predictive and preemptive power it promises. Terrorism succeeds by invading the host system and turning its resources against itself. As Bacon and the IAO motto scientia est potestas reminds us, that bargain confers great power to the government. In the information age, knowledge is power indeed, and total knowledge is total power.

The aspect of TIA that stimulates strong resistance among some citizens is the "T" for "Total." Because the system mines normal streams of data in order to search for potential terrorist operations, it cannot be selectively targeted in advance. TIA looks for hidden patterns of activity. This is distinct from investigations that move ahead based on probable cause to gather information about specific individuals or groups. TIA is a design to operate with total streams of information: everyone’s credit card records, everyone’s telephone calls, everyone’s travel plans, and so on. TIA does not include a plan to maintain a dossier on every U.S. citizen. In fact, the initial design will include measures to separate individuals from data. Still, the aggregate record of every U.S. citizen’s activities will be used to generate the results. To many civil libertarians, such total data mining is the information highway analogue to random roadblock and search checkpoints on public highways, which the Supreme Court ruled (6-3) unconstitutional (Sealey, 2000).

The Association for Computing Machinery U.S. Public Policy Committee (USACM) voiced objections regarding TIA to the Senate Committee on Armed Services (Simons & Spafford, 2003). To support their position: “the overall surveillance goals of TIA suffer from fundamental flaws that are based in exceedingly complex and intractable issues of human nature, economics and law. Technological research alone cannot make a system such as TIA viable,” the USACM Chairs cite four areas of major concern:

1) Security risks: a centralized data system such as TIA intends to use will be vulnerable to hackers, criminals, and terrorists. Concentrating such sensitive data might make us less secure.

2) Privacy risks: By definition, surveillance compromises privacy. Coupled with the veil of secrecy within which TIA will operate, the plan creates a breach of existing privacy standards that technology cannot solve.

3) Economic risks: Consumers and companies will seek alternates to the existing Internet in order to avoid TIA scrutiny. This may lead to exclusion of U.S. companies from important markets, similar to the European Union ban on genetically modified foods.

4) Personal risks: Even the best case scenario for a pattern recognition system will generate millions of false positives. Innocent citizens may be tagged as possible terrorists, with no recourse to correcting the erroneous data.

USACM regards TIA as creating certain risks for uncertain gains. The absence of a legal and political oversight mechanism for the Information Awareness Office underscores the depth of that risk. We shall have to take the IAO at its word regarding the success of the program.

Proponents of TIA argue that the system will be designed to mask individual identities, that it will be subject to existing privacy protections and limits on investigation, that it will only be used to detect terrorists, and that the technology is separate from and neutral to the policies guiding its use (Aldrich, 2002). It is clear, however, that TIA is designed not as a single tool for a specific purpose, but as a technical infrastructure for intelligence and law enforcement information. Director of the Information Awareness Office (IOA) John Poindexter observes that TIA is “the overarching program that binds IAO’s efforts together” (Mayle & Knott, 2002). Such efforts include automated language translation, HumanID (e.g., identifying individuals by characteristic body movements), and BioSurveillance (e.g., identifying individuals by odors). The Total in “Total Information Awareness” refers both to the universality of information (everyone’s records) as well as the broadest feasible range of data streams. The ultimate success of TIA will be the real-time aggregation of all electronic information available about everyone. This centralized scrutiny is what leads many to see the Total in TIA as a step to Totalitarian.

A scalable TIA will be able to assimilate any existing data stream. To understand the scale to which Admiral Poindexter’s project ultimately aspires, one must consider the realm of available data streams. The U.S. Secret Service contracted Image Data LLC in 1998 to produce a national database of driver’s license photographs (Cabell, 1999). Numerous US states and several countries use electronic toll collection systems that scan barcodes on windshield tags from cars in motion. The resulting data is used to generate toll bills sent to drivers (Knowles, 2000). The FCC requires cell phone...
networks to be able to know the caller’s number and physical location to aid 911 emergency operators (Zhao, 2002). These few projects provide a rudimentary list at the beginning stages of the constant and minute collection of data in 21st century culture. Any object, action, or state that can be quantified and measured is a candidate for data collection. TIA is a system designed to use any and all data streams. Even with the short list of existing data streams, TIA would enable government agencies to query the history of an individual’s purchases, reading habits, conversations, and physical movement. Of course, as proponents note, the capability to compile such data is different from the intent and legal power to do so. It is well, then to consider how the laws limiting uses of a technical capability fare in the State of Terror.

The uses of raw and processed data streams such as those to be centralized by TIA are limited only by intent and policy. Whatever the stated intentions of a data mining project, we must consider the implications of uses under other conditions, especially uses that are political, commercial, scientific, personal, and criminal. Understanding the consequences of the misuses of information is crucial because where information exists, there are also constant social and psychological pressures to use it. These pressures to use information are describable via three principles: (1) Information not used is opportunity wasted, (2) Laws change, agendas persist, (3) Flexible descriptions enable mission creep. These principles practically ensure that whatever the stated intentions for an information technology, unintended uses will emerge. Consider some cases of information re-purposing as exemplars of these three principles.

**Information not used is opportunity wasted**

The book of Genesis records the first instance of a restrictive information policy. Yahwe gave Adam and Eve free reign over all, with the exception of the tree of knowledge (a sex and death database). The forbidden fruit, of course, became the most desired object in the garden. It is not merely the restrictions that create interest in information, it is also the appeal of the unknown.

This principle was recently exemplified in the state of terror created by the snipers who shot 13 people in October 2002. The FBI set up a hotline to gather tips from the public with the instruction: “to make sure that they provide substantive information relating to the sniper attacks; but not theories, opinion or unrelated information which needlessly tie up the tip-line” (Murray, 2002). Since so few of the tips aided the investigation, there must have been a lot of unrelated information. Unrelated though it may be, it will not go to waste. One month after apprehending the snipers, Montgomery County, Maryland police created “a three-officer task force to sift through the more than 70,000 tips received during the sniper investigation, hoping the information will lead them to people who are possessing guns illegally.” Information solicited specifically for the sniper investigation is re-purposed for other law enforcement tasks. Capt. Nancy Demme of the Montgomery County police makes the rationale for this change clear: “There’s a lot of information. We would be negligent if we threw it to the wayside because it didn’t have to do with the sniper.” Several other jurisdictions are similarly putting the FBI hotline tips to work. It seems likely that the uses of the tip information will exceed gun law enforcement as well.

Whatever the reasons for gathering information, once held it is a valuable resource that may serve other purposes. Generally we regard the non-use of information as wasteful, even immoral. Once TIA data are gathered, we can be sure that the desires to put them to initially unintended purposes will be powerful. Maximizing the potentials of a universal database for the sake of political power may even be regarded by a righteous few as their moral duty. Our information technologies must be designed to thwart future appropriations of data power.

**Laws change, agendas persist**

Civil law and its interpretation is relative to conditions. The state of terror will yield new laws and override old policies. Such conditions are opportunities for agendas that have been blocked prior to the emergency. It is crucial to maintain linkage with prior agendas, however they are repackaged. Many marveled at the swift passage of the Patriot Act (H.R. 3162) passed October 25, 2001. Subtitled, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, the new laws are largely old military and law enforcement agendas refocused on terrorism. An example is Carnivore, the FBI email and web-tapping tool.

Carnivore began as Omnivore in 1977 and possibly before as Etherpeek. It is a hardware-software combination that acts as a packet-sniffer when installed on an Internet Service Provider (ISP) or network. Carnivore is veiled in secrecy, despite the Freedom of Information Act disclosures won by the Electronic Privacy Center in 2000. Several ISPs resisted FBI efforts to install Carnivore on their network routers. A major complaint against Carnivore by privacy advocates and computer scientists is the design to filter and archive all of the packets (email and web requests) that pass through it. Armed with a court order, the FBI would then have allowance to decode the data related to an individual under investigation. Once decoded, the FBI could read all of that individual’s email and view the web pages that they visited and web searches they conducted. In many ways this is like a wiretap on a telephone. The major difference is that all of the information traffic is monitored and archived. This is like a wiretap on the phone company switches to collect everyone’s calls. Some computer experts object that such a capture-it-all-and-sort-it-later strategy is unnecessary and sloppy. Privacy advocates
object that Carnivore amounts to unlawful search and seizure of online communications en masse. The FBI presents Carnivore as a safe and suitable tool;

The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept. This type of tool is necessary to meet the stringent requirements of the federal wiretapping statutes. (FBI, 2000).

The legal and conceptual battle over Carnivore has not been by objections to the FBI using a wiretap on email. Rather, the major objections involve the methods allegedly used by Carnivore to capture and archive all unfiltered traffic. Apparently, Carnivore may ignore unfiltered traffic, but it does not discard that traffic. Once through the Carnivore black box, all email packets become part of the archive. The desired bytes may be surgically removed from that body of data, but the body remains in state. (EPIC, Test Report of June 2000).

On September 11, 2001 the battle over Carnivore changed course. Within hours of the 9-11 destruction, the FBI was installing Carnivore on numerous ISPs, including some that had previously resisted (Cha & Krim, 2001). The Patriot Act changes the Carnivore name to DCS1000 and eliminates the need for probable cause to be established in advance of its installation and use. The Patriot Act leaves restrictions on who can be monitored open, so possibly any subscriber to the ISP identified by law enforcement as relevant to an investigation could be targeted. Given that DCS1000 (a.k.a. Carnivore) sniffs and saves all that passes through it, email and web use surveillance may be executed retroactively. ISPs giants such as AOL and Earthlink are cooperating with the FBI. Pursuant to the Patriot Act, the majority of the email users in the US may now be under e-wiretap.

Another FBI surveillance project, Magic Lantern, is a Trojan Horse virus similar to the Love Bug virus that nearly brought down the Internet in May 2000. Unlike destructive viruses that self-replicate out of control, Magic Lantern lives quietly inside the host computer in order to do one task: copy keystrokes made on the computer and report them to the FBI. Magic Lantern is especially useful in cracking users of encryption software, since it monitors the keystrokes before they are encrypted. Possibly the program can also steal and reveal encryption keys from the target computer. An important question is how Magic Lantern will be distributed, as the Trojan Horse must be contained within some other legitimate software package. It also creates a curious position for anti-virus software producers such as Symantec and McAfee (Jackson, 2001). The program can lie dormant until given the command to go to work, triggered either by the use of encryption software or perhaps a cuing order from outside. The FBI denied the existence of Magic Lantern up to 2001 (About.com., 2003). The Patriot Act loosens wiretap authority broadly, thus allowing expanded uses for Magic Lantern.

Technologies such as Carnivore and Magic Lantern are stages in the traditional efforts of law enforcement and intelligence agencies to gain access to individual communications. Many of the issues regarding privacy and law enforcement technique remain even when the technologies change. The notable point that these technologies provide is the re-framing of them as terrorist fighting tools. These programs were developed for general purpose law enforcement use. They were not designed specifically in response to terrorism. Yet, after 9-11, the technologies, methods, and policies that can be used against terrorists are commonly described as though designed in response to terrorism. In the State of Terror all attention is turned to the terrorist and the issues of concern over technologies, methods, and policies are overridden. Prior agendas, especially those blocked by legal challenge, are repackaged in terms of terrorism and use the State of terror as an opportunity.

TIA is a prior agenda with a new charge; it is an outgrowth of the Genoa project, an intelligence coordination program developed for DARPA in 1997. Syntek was the developer, with John Poindexter as the project director. Poindexter's new role as Information Awareness Office Director overseeing TIA is a continuation of the (at least) six-year-old project.

Depending on conditions, the laws will change again. The uses of TIA and other data mining systems may hold limits under current law, but their agendas and data will persist. The question to be considered is how the agenda and archives of TIA may be used under more authoritarian laws than even the Patriot Act. This is the basis of concern for many critics of mass data mining. TIA, as presently envisioned, provides the means and opportunity for abuses of privacy and human rights by future governments. Present law can neither anticipate nor prevent such abuses. Consequently, the limits to power must be intentionally designed into the technology.

**Elastic descriptions enable mission creep**

Once a technology or policy has been identified as a weapon against terrorism, it is important to follow closely what happens to the definition of terrorism. Changes in the concept of terrorism and related terms can have immense impact on what political authorities may do consistent with their own dictates. The assurance that TIA will be used only to fight terrorism is a common response to its critics. Yet, even as these assurances are given, the definition of terrorism is undergoing change. The 2001 Patriot Act redefines terrorism in a broad enough fashion to include violent protest and computer crime. Since legal definitions frequently broaden their scope, the current redefining of terrorism points to future widening of the total surveillance net.

The Patriot Act constitutes a major shift in the legal definition of terrorism. The shift is significant since the Patriot Act delineates what law enforcement agencies may do and what individuals may not do. To see the change in meaning, begin with the definition of terrorism adopted by the U.S. State Department in its 2000 "Patterns of Global Terrorism" report:

No one definition of terrorism has gained universal acceptance. For the purposes of this report, however, we have chosen the definition of terrorism contained in Title 22 of the United States Code, Section 2656f(d). That statute contains the following definitions: The term “terrorism” means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience … The U.S. Government has employed this definition of terrorism for statistical and analytical purposes since 1983 (U.S. Department of State, 2000).

This definition presents a familiar picture of terrorism as politically motivated violence directed against civilians or non-combatants. Compare that workhorse definition from U.S. law to the new definition stipulated in the Patriot Act.

SEC. 802. the term ‘domestic terrorism’ means activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; appear to be intended— to
intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnaping; and occur primarily within the territorial jurisdiction of the United States. (HR 3162, 2001).

The new legal definition of terrorism excludes the necessity of violence in the acts, replacing “politically motivated violence perpetrated against noncombatant targets” with “activities that involve acts dangerous to human life that . . . appear to be intended— to intimidate or coerce a civilian population.” The new definition does not require that terrorism be targeted against civilians or non-combatants. Under the new definition, terrorism may include crimes against property and perhaps certain forms of civil disobedience. The distance from the former legal definition becomes even wider when the Computer Fraud and Abuse Act that was introduced as a rider to the Patriot Act adds to the list of terrorist activities.

An act calculated to influence or affect the conduct of government by intimidation or coercion or to retaliate against government conduct AND violates 18 USC §1030(a)(1) accessing restricted or classified information on computers that require protection for reasons of national security, national defense or §11(y) of Atomic Energy Act of 1954 with reason to believe that the information could injure US or advantage a foreign nation, and who willfully communicates the information to one not entitled to it. (EFF, 2001).

A wide variety of computer crimes and hacking will qualify as terrorism under this statute. The concept of terrorism has departed from the violence of bus bombings and hijacking onto the transmission of restricted information. It is clear to see how this extended definition of terrorism may impact the mission of mass data mining and surveillance systems such as TIA and Carnivore. The existing law prescribes a vastly broader role for TIA than our common notions of terrorism anticipate.

Elastic descriptions are political works of art. Admiral John Poindexter, Director of the Information Awareness Office and former Senior Vice President of Information Systems at Syntek (prime contractor for TIA) knows a great deal about the elasticity of meaning. His Syntek curriculum vitae notes:

As the National Security Advisor to President Ronald Reagan, VADM Poindexter played a major role in world events including: support for the democratic resistance in Nicaragua, and an attempt to begin rationalization of U.S. relationship with strategically important Iran.

For his efforts in those “major roles,” Poindexter received six felony convictions (Syntek, 2001). A little re-description goes a long way.

**The War on Criminal Extremists**

Given the three principles demonstrated above — the compulsion to use all available data, the persistence of national security agendas, and the power of elastic description — we are in position to identify some specific implications of TIA technology. City, county, and state police department records and reports are obvious contributors to the TIA data stream. Many police departments already use database systems such as Orion Scientific Systems TaskForce: “a suite of software tools enabling law enforcement with the ability to collect, evaluate, analyze, and share information utilizing techniques that will enable the user to access and share realtime information from anywhere at anytime “ (Orion Scientific Systems, 2003). The Denver Police Department has been using TaskForce to compile profiles on “Criminal Extremist” groups and their members. The American Civil Liberties Union (ACLU) recently revealed that the Denver Police Department has conducted a covert program of surveillance and infiltration into 208 groups and some 3,200 individuals. These groups include The American Friends Service Committee (a Quaker pacifist organization), Amnesty International (AI), the Green Party, Colorado Coalition for the Prevention of Nuclear War, the American Indian Movement (AIM), and academic conferences. For at least four years, the Denver Police Department has deployed undercover officers into meetings and demonstrations of these groups for the purpose of monitoring plans of the groups and monitoring individual members. The individuals have extensive files detailing their physical descriptions, employment, family members, home address, and automotive license plates. What these subjects say and do at meetings is recorded and filed in the data mine.

The Denver Police intelligence program was secret enough that Denver Mayor Webb claims not to have known of it until some of the files were leaked to some of the subjects of investigation. Denver Public Safety Department spokeswoman C.L. Harmer said people named in the files were not considered criminals and the files were collected because legal gatherings are sometimes the scene of illegal actions. “Law-abiding groups sponsoring lawful assemblies can be unwitting magnets for unlawful activity,” she said, “If you go to a peaceful demonstration, is your name going to come up when you get a traffic ticket? The answer is no, because the data isn’t shared,” she said, “I don’t think this is a retreat to the era of J. Edgar Hoover.” Harmer said that although the intelligence-gathering started before the terrorist attacks, the attacks illustrated the need for such files (Associated Press, 2002).

Harmer’s comments underscore the crucial point: the danger to civil liberties from police political spying is markedly increased as that information becomes shared among government agencies. TIA is a system specifically designed to collect and share such information as that collected by the Denver Police. Some municipalities (Seattle, San Fransisco, Portland) officially restrict police surveillance of lawful activities, though in the State of Terror the few barriers to political spying are easily passed over. The New York Police Department (NYPD) is seeking the power to conduct political surveillance without authorization from the official three-member panel set up to provide oversight after NYPD abuses in the 1970s (Pollitt, 2003). TIA will surely be taking advantage of that data stream.

That local law enforcement is transformed into secret political police is a clear threat to civil liberties. That lawful political organizations such as Nobel Peace Prize laureates, Amnesty International, and the American Friends Service Committee are categorized by secret political police as “criminal extremist” groups is frighteningly absurd. That a legal national political party, the Green Party, is monitored by secret political police is Stalinist. The prospect that such information will be combined with official and commercial data streams is outright totalitarian. The KGB or STASI could not rival this U.S. surveillance totality.

**Qui custodiet ipsos custodes?**

This much is clear: a system like TIA has immense potential for abuses against basic freedom and a functioning system like TIA is inevitable. Why is it inevitable? Because data mining...
systems such as TaskForce are already in use in law enforcement offices around the world. TIA is a grand design for the cutting edge in surveillance of a populace, but even if it is never built, the existing data mining will continue to improve and eventually be networked into larger systems. Thus the primary issue at hand ought to be how to manage such developments to minimize their threat to freedom and human rights. Two aspects foremost in that issue are: requiring oversight to increase accountability and requiring technical designs that minimize the abuse potential.

Sufficient monitoring of a nationwide surveillance data mining operation will require oversight by both judicial and legislative bodies, as well as competent citizenry. The U.S. constitutional democracy replies on adequate checks and balances among diverse interests. Mass scale data mining will require diverse and redundant checks and balances. TIA is the information technology equivalent of a nuclear missile arsenal. Unexpected consequences and outright errors are so severe that extreme measures to mitigate risk are called for. Nuclear weapons have redundant command and control systems to prevent accidents and abuses. TIA should hold similar standards of redundancy and diversity in the command and control of information. This requires that some levels of secrecy in the TIA application must be removed.

A likely objection to the above argument is to extend the analogy by pointing out that nuclear weapons are maintained under strict secrecy, the very condition that I argue needs to be modified in regards to TIA. This extension actually strengthens the analogy since nuclear armed forces are capable of maintaining adequate security while remaining subject to civilian control and oversight. The key to oversight is to diversify the controls so that they are not monopolized by an insular political element. In the case of the military, this means opening information and policy making to non-military authorities. In the case of TIA, this means opening information, policy, and audit trails to interests outside of law enforcement and the military.

Perhaps the most vital specification for the control of TIA is the need for record keeping about its operations. There should be a hard-coded (non-optional) means to audit applications of the TIA information. Moreover, the very technology used to mask identities from the data might be used to generate abstracts of TIA operations, without giving away law enforcement case specifics. Citizens, therefore, should have the capacity to determine how many times TIA is used and for what general purposes. Thus, uses of TIA exceeding the intended application to catch terrorists (however that is currently defined) will be detectable and future abuses may be preventable.

Whether there are technical solutions to the present TIA and similar systems, to prevent them from becoming an Orwellian nightmare is an unknown. To DARPA's credit, part of the TIA project involves testing the firewall between individual identities and the mass of data collected. Dr. Teresa Lunt of Xerox PARC is the chief scientist in a research effort to protect identities from unauthorized scrutiny in data mining operations. The task is a great one because there are many ways to collate and trace data back to its source; the information trails that we individually generate are tied to our identities. As well as masking identities from data, Lunt is devising an audit trail to monitor uses of TIA information. An "audit trail that could be examined by third parties, if appropriate, to look for potential abuses by analysts who have access to this data. At some future point, there could be a law that allows people to seek redress from the government if they feel their privacy’s been violated" (Hoffman, 2003).

Lunt’s approach to creating a TIA audit trail is a positive development, given appropriate oversight of the audit data. Still, Lunt does not express confidence that her work is high in the priorities of the IAO; “Nobody’s made a commitment to use this technology,” Lunt said. “When we have a technology and it’s proposed for some very critical life-and-death application, I would feel a lot of pressure at that point. I don’t yet feel like the world is on my shoulders” (Hoffman, 2003).

**Potentia Maledicta**

The IAO emblem shows an eye in a pyramid casting its gaze over the earth entire with the motto “scientia est potentia.” The eye in a pyramid is a variant of the image on the Great Seal found on dollar bills. On the Great Seal the image symbolizes the omniscient view of God overlooking the work of the United States government. In the IAO emblem, the U.S. government replaces God as the all-seeing observer. This symbolic shift signals the significance that TIA and related technologies bode for us. Philosophers should be foremost among the thinkers who take these matters as a concern for serious study. Increased understanding of how privacy and identity may be impacted by mass data mining is vital. Philosophers with awareness of computing issues are particularly critical players in this matter. I urge all who read this to study, write, and speak on issues related to mass data mining by the government. If knowledge is power itself, then we had all better gain all the knowledge we can about Total Information Awareness.

**Notes**


--- 107 ---


http://netsecurity.about.com/library/weekly/aa121901a.htm


Total Information Awareness Homepage  http://www.darpa.mil/iao/TIASystems.htm

