

CREATING A FEDERAL DATABASE:
THE TOTAL INFORMATION AWARENESS PROJECT
A Module for Democracy/Civic Mission
Classrooms

Constitutional Rights Foundation Chicago
407 South Dearborn, Suite 1700
Chicago, Illinois 60605-1119
<http://www.crfc.org> ♦ crfc@crfc.org

Adapted from: *Safety and Freedom in Post-September 11 America: 2003 Illinois Youth Summit Resource Guide for Students and Teachers*. Copyright © 2003, 2006 Constitutional Rights Foundation Chicago. May be reproduced for educational use only.

"Total Information Awareness": Creating a Federal Database

Overview

In 2002, an experimental Pentagon research project called Total Information Awareness (TIA) was being created under leadership of the Defense Department's Information Awareness Office (IAO). The TIA program objective is to aid the United States in detecting, classifying and identifying foreign terrorists in order to successfully preempt and defeat terrorist acts.

This unit examines the Total Information Awareness project and some of the issues it raises for Americans about privacy, freedom, and security in the wake of the attack of September 11, 2001. This unit also defines and explains public policy – what it is and how it works. The unit introduces GRADE, a strategy for evaluating this and other public policies.

Focus Questions

- § Will the Total Information Awareness project be an effective security measure to reduce the threat of terrorism?
- § Is the Total Information Awareness project an acceptable use of personal information about U.S. citizens and residents by the federal government?
- § Should the U.S. Government develop the Total Information Awareness project?

Objectives

- < Provide information about the scope and purpose of the Total Information Awareness project.
- < Highlight the difficulties faced by the federal government in preventing terrorist attacks within the United States without coordinated access to data located in multiple databases.
- < Identify concerns surrounding personal information that would be accessible through a coordinated search structure maintained by the federal government.
- < Generate a working definition of public policy, supply tools for analyzing policy in order to form an educated decision, and promote recognition of the impact of public policy and how to affect policy decisions.
- < Develop and support a reasoned position on the creation of the Total Information Awareness project.

Materials

- A: Reading: What Is Total Information Awareness?
 - B: Source: Defense Advance Research Projects Agency's (DARPA) Office of Information Awareness (OIA) and Total Information Awareness Project
 - C: Activity: National Security and Personal Privacy: A Human Graph
 - D: Questions: National Security and Personal Privacy
 - E: Activity: Developing Total Information Awareness: A Presidential Commission
 - F: Strategy: Looking at Public Policy: G R A D E
 - G: Taking a Stand: Position Paper on Total Information Awareness
- Creating a Federal Database: Selected Community, Print, and Internet Resources

A: Reading: What is Total Information Awareness?

In addition to the terrible loss of life and damage to property, the attacks of September 11 were a failure of U.S. intelligence. Information about al-Qaeda members and other groups hostile to the United States was not shared among the Federal Bureau of Investigation, the Central Intelligence Agency, the Immigration and Naturalization Service, and other federal agencies. Trends and possible threats, such as the use of commercial airliners as lethal missiles, were not anticipated or adequately appreciated. Even information that people realized was important – including the Phoenix FBI office's memo about flight school students – failed to reach the people who might have been able to fit it into a larger pattern. People inside and outside the federal government referred to this problem as a failure to “connect the dots.”

One major challenge to terrorist detection today is the inability to quickly search and correlate data – information – from the many databases already maintained legally by U.S. intelligence, counterintelligence, and law enforcement agencies. How can all this information be reviewed in time? And how can the privacy of ordinary U.S. citizens be protected in the process?

DARPA and Total Information Awareness

Following World War II, the federal government created the Defense Advanced Research Projects Agency, or DARPA, with the mission of researching and demonstrating innovative technologies to solve national-level problems. Since its creation, DARPA has tackled many high-risk research efforts, and its work has resulted in significant advances in using technology. Many important and existing information technologies – including the Internet – began as advanced DARPA research projects.

Following the attacks of September 11, 2001, DARPA created the Information Awareness Offices (IAO) to help conduct research into advanced information capabilities that will give the United States the ability to “detect terrorist groups planning attacks against American citizens, anywhere in the world.” One new program to meet that goal is Total Information Awareness (TIA). According to DARPA, “the goal of the Total Information Awareness (TIA) program is to revolutionize the ability of the United States to detect, classify and identify foreign terrorists – and decipher their plans – and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts.”

Total Information Awareness — How It Works

The objective for Total Information Awareness is to create a counter-terrorism information system that: “(1) increases information coverage by an order of magnitude, and affords easy future scaling; (2) provides focused warnings within an hour after a triggering event occurs or an evidence threshold is passed; (3) can automatically queue analysts based on partial pattern matches and has patterns that cover 90% of all previously known foreign terrorist attacks; and, (4) supports collaboration, analytical reasoning and information sharing so that analysts can hypothesize, test and propose theories and mitigating strategies about possible futures, so decision-makers can effectively evaluate the impact of current or future policies and prospective courses of action” (DARPA).

TIA will consist of three parts. (1) Language translation technologies will allow for the rapid translation of foreign language publications so that intelligence analysts can quickly search for clues about emerging terrorist acts. Many in the intelligence community believe that evidence of terrorist activities can be found in these “open source” foreign language

publications. (2) Data search and pattern recognition technologies is based on the idea that terrorist planning activities or attacks could be discovered by searching for clues in "transaction data," such as applications for passport applications, visas, work permits, and drivers' licenses; automotive rentals; and purchases of airline tickets and chemicals. TIA might allow intelligence analysts to connect these transactions with specific events, such as arrests or suspicious activities. (3) Advanced collaborative and decision support tools will help solve existing coordination problems by enabling analysts from one agency to effectively collaborate with analysts in other agencies.

Security with Privacy: The Technical Challenges

The technical challenges to Total Information Awareness are enormous. Existing government and commercial databases vary greatly in how they are built, what data they store, and how those data are protected. Federal agencies often do not share data or are prohibited by law from doing so.

In its December 2002 report "Security with Privacy," the Information Science and Technology (ISAT) study group of the independent Institute for Defense Analyses addressed the technical problems for meeting the challenge of greater data search capacity and improved personal privacy. "At the heart of a privacy system will be the ability to express rules for handling private information. These rules must be readable both by machine (so that they can be electronically enforced) and by humans (who can check the rules for accuracy). Similarly, compliance to these rules must be checked (and checkable) both automatically and by people."

ISAT identified three technical strategies to meet these challenges. Selective revelation is "a method for minimizing exposure of individual information while supporting the continuous analysis of all data." Selective revelation means revealing to intelligence analysts only statistics and categories of interest but not any data that would directly or indirectly identify a person.

For example, an analyst might issue a query asking where there is any individual who has recently bought unusual quantities of certain chemicals, and as rented a large truck. The [computer query] could respond by saying yes or no, rather than revealing the identify of an individual. The analyst might then take that information to a judge or other appropriate body, seeking permission to learn the individual's name or other information about that individual ["Security with Privacy," p. 10].

In this way, selective evaluation puts a "security barrier" between the analyst and the data.

Another strategy ISAT identified is strong audit or "watching the watchers." While nearly everyone recognizes the importance of strong audits – where everyone who comes in contact with data is "audited" or checked – ISAT reports that "these systems themselves pose a substantial challenge. Audit data will be voluminous and highly sensitive. How can we find instances of inappropriate queries? ... This hall of mirrors presents a number of technical challenges" [p. 13].

Rule processing technologies – how information is labeled and what level of protection it receives – are another important strategy because this kind of analysis combines data from diverse sources. Each data source has particular privacy limits. Information also varies greatly in quality and accuracy. Labeling data so that it is recognized and sorted correctly is tremendously difficult. And "even a new information system will likely build on substantial amounts of (accurately or inaccurately labeled) previously existing "legacy data."

Nevertheless, ISAT concluded that the problem of protecting personal privacy needed study now, not only because of issues raised by national security but also because of the "explosion"

in commercial data collection and exploitation and because this is a “ripe time to build on recent scientific advances.” “In any case, the deployment of powerful distributed information system, as envisioned by the Transportation Security Agency, the FBI, and TIA will need powerful privacy mechanisms or else the American people (rightly so) will refuse to accept deployment” [p. 7].

Some experts in technology have doubts that TIA can work. “The kind of things they are looking for are hard to find,” according to Herb Edelstein, president of data-mining company Two Crows. “It’s not clear this is an economically valuable way to fight terrorism” [“Total Info System Totally Touchy,” *Wired News*, December 2, 2002]. “This wouldn’t have been possible without the modern Internet, and even now it’s a daunting task,” according to Dorothy Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School in Monterey, California. “Do we really know enough about the precursors to terrorist activity? I don’t think we are there yet” [“Many Tools of Big Brother Now in Place,” *New York Times*, December 23, 2002].

Too Much Like “Big Brother”?

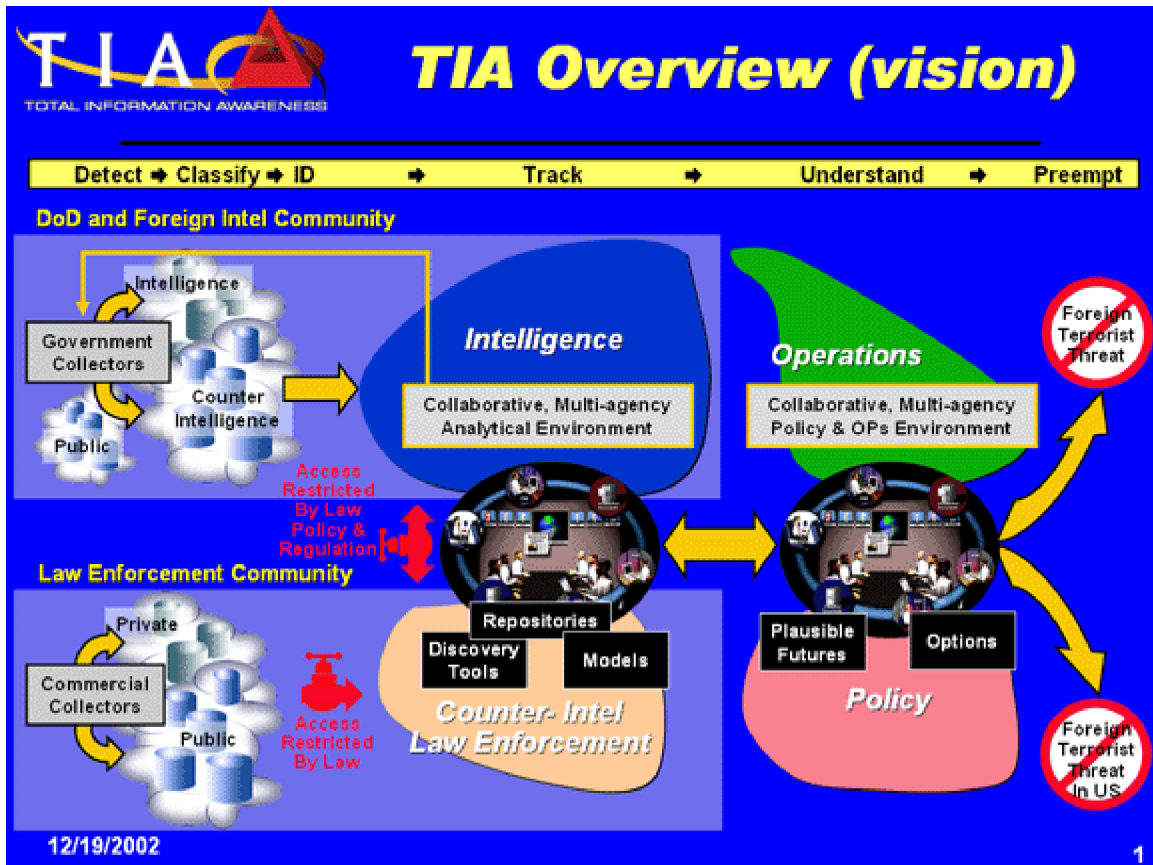
Yet perhaps the greatest challenge facing Total Information Awareness is the privacy concerns of ordinary Americans. Regardless of party, Americans across the political spectrum are very concerned with limiting how personal information is accessed and used by the federal government. Such information is currently protected, sometimes very strictly and often quite loosely, by a complicated web of state and federal laws.

The U.S. Department of Defense, which controls DARPA, has said that TIA “will not violate the privacy of American citizens, the Department has safeguards in place. In addition, IAO will research and develop technologies to protect the system from internal abuses and external threats. The goal is to achieve a quantum leap in privacy technology to ensure data is protected and used only for lawful purposes.” Defense Secretary Donald Rumsfeld has downplayed concerns about TIA. “You have some very talented people taking some small fraction of the taxpayers’ money and investing it to see if we can’t find ways to do things better” (“Rumsfeld Says Don’t Sweat DARPA Info Awareness Experiment,” *Associated Press*, November 18, 2002).

Gene Healy of the Cato Institute disagrees. “If the history of military surveillance of civilians is any indication, accepting that assurance amounts to the triumph of hope over experience” [Beware of Total Information Awareness, January 20, 2003]. In fact, many Americans see the Total Information Awareness program as “Big Brother,” the crushing totalitarian state described by George Orwell in his novel 1984. “Our privacy has actually been protected by the fact that [information collected about Americans] still remains scattered across many different databases,” according to Jay Stanley and Barry Steinhardt of the American Civil Liberties Union (“Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society,” January 2003). This “pent-up capacity for surveillance... will be realized if the government... gain[s] the ability to draw together all this information.” Groups as diverse as the conservative Eagle Forum and liberal People for the American Way oppose the idea.

This opposition has found expression in Congress. In January 2003, the U.S. Senate voted to bar deployment of TIA within 60 days of enactment of the bill unless the Defense Department reported in detail on its impact on privacy and civil liberties and the likelihood of its success in stopping terrorists. The research could also continue if President Bush certified to Congress that a halt “would endanger the national security of the United States.” While the future of the Total Information Awareness project is still uncertain, the issues of greater security and privacy – in a world of increased data and danger – will remain for the foreseeable future.

B: Source: Defense Advance Research Projects Agency's Office of Information Awareness and Total Information Awareness Project



Program Objective

The Total Information Awareness (TIA) program is a FY03 new-start program. The goal of the Total Information Awareness (TIA) program is to revolutionize the ability of the United States to detect, classify and identify foreign terrorists – and decipher their plans – and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts. To that end, the TIA program objective is to create a counter-terrorism information system that: (1) increases information coverage by an order of magnitude, and affords easy future scaling; (2) provides focused warnings within an hour after a triggering event occurs or an evidence threshold is passed; (3) can automatically queue analysts based on partial pattern matches and has patterns that cover 90% of all previously known foreign terrorist attacks; and, (4) supports collaboration, analytical reasoning and information sharing so that analysts can hypothesize, test and propose theories and mitigating strategies about possible futures, so decision-makers can effectively evaluate the impact of current or future policies and prospective courses of action.

Program Strategy

The TIA program strategy is to integrate technologies developed by DARPA (and elsewhere as appropriate) into a series of increasingly powerful prototype systems that can be stress-tested in operationally relevant environments, using real-time feedback to refine concepts of operation and performance requirements down to the component level. The TIA program will develop and

integrate information technologies into fully functional, leave-behind prototypes that are reliable, easy to install, and packaged with documentation and source code (though not necessarily complete in terms of desired features) that will enable the intelligence community to evaluate new technologies through experimentation, and rapidly transition it to operational use, as appropriate. Accordingly, the TIA program will work in close collaboration with one or more U.S. intelligence agencies that will provide operational guidance and technology evaluation, and act as TIA system transition partners.

Technically, the TIA program is focusing on the development of: 1) architectures for a large-scale counter-terrorism database, for system elements associated with database population, and for integrating algorithms and mixed-initiative analytical tools; 2) novel methods for populating the database from existing sources, create innovative new sources, and invent new algorithms for mining, combining, and refining information for subsequent inclusion into the database; and, 3) revolutionary new models, algorithms, methods, tools, and techniques for analyzing and correlating information in the database to derive actionable intelligence.

More Information

The Defense Advanced Research Projects Agency's (DARPA) mission is to research and demonstrate innovative technologies to solve national-level problems, such as the grave terrorist threat which our nation faces. DARPA created the Information Awareness Office (IAO) in response to September 11, 2001, to research, develop, and demonstrate innovative information technologies to detect terrorist groups planning attacks against American citizens, anywhere in the world.

Contrary to some recent media reports, IAO is not building a "supercomputer" to snoop into the private lives or track the everyday activities of American citizens. Instead, IAO is developing an experimental prototype system that consists of three parts — language translation technologies, data search and pattern recognition technologies, and advanced collaborative and decision support tools. Together, these three parts comprise the Total Information Awareness (TIA) project.

The language translation technologies will enable the rapid translation of foreign language publications and give intelligence analysts the capability to quickly search for clues about emerging terrorist acts. The intelligence community believes it can find evidence of terrorist activities in open source foreign language publications. Rapid translation technologies will help intelligence analysts search a significant amount of material in a much shorter period than is possible today.

The research into data search and pattern recognition technologies is based on the idea that terrorist planning activities or a likely terrorist attack could be uncovered by searching for indications of terrorist activities in vast quantities of transaction data. Terrorists must engage in certain transactions to coordinate and conduct attacks against Americans, and these transactions form patterns that may be detectable. Initial thoughts are to connect these transactions (e.g., applications for passports, visas, work permits, and drivers' licenses; automotive rentals; and purchases of airline ticket and chemicals) with events, such as arrests or suspicious activities. For this research, the TIA project will use only data that is legally available and obtainable by the U.S. Government.

A major challenge to terrorist detection today is the inability to quickly search and correlate data from the many databases maintained legally by our intelligence, counterintelligence, and law enforcement agencies. The collaborative reasoning and decision-support technologies will

help solve existing coordination problems by enabling analysts from one agency to effectively collaborate with analysts in other agencies.

Today, the full TIA prototype exists only as a vision. The project is in its first year of an anticipated 5-year research effort. During the first 36 months, a range of ideas will be developed via limited demonstrations and preliminary prototypes. During the final 24 months, the most promising research avenues will be extended to support production of a scalable leave-behind system prototype. If the project is successful, the Department of Homeland Security will consult with Congress to determine whether the TIA system should be implemented for domestic use. The DoD will consult with Congress on how to best implement the system for protection of U.S. forces overseas.

The DoD recognizes American citizens' concerns about privacy invasions. To ensure the TIA project will not violate the privacy of American citizens, the Department has safeguards in place. In addition, IAO will research and develop technologies to protect the system from internal abuses and external threats. The goal is to achieve a quantum leap in privacy technology to ensure data is protected and used only for lawful purposes.

Some individuals have questioned the role of the DoD and DARPA in this area. In its 54-year history, DARPA has undertaken numerous high-risk research efforts that led to significant capabilities. Many existing information technologies-including the Internet-started as advanced DARPA research projects. IAO follows a similar path of technical innovation with its research into advanced information capabilities that will give the United States a decisive edge in the global war on terrorism. All Americans share the frustration associated with vague warnings of terrorist threats. It is believed that IAO and its TIA project will help the U.S. Government reduce those generic reports to advance notice of specific threatening acts.

Text and Graphic from: Information Awareness Office Programs, Defense Advanced Research Projects Agency, United States Department of Defense, <http://www.darpa.mil/iao/TIASystems.htm> and <http://www.darpa.mil/iao/iaotia.pdf>

C: Activity: National Security and Personal Privacy: A Human Graph

This activity is designed to introduce participants to the different issues raised by the federal government's Total Information Awareness (TIA) project, and to help them realize how they feel and where they stand on the privacy of personal information in the face of threats to national security and their own safety.

Procedures

- § Explain the purpose of this activity. Then create a line – either by pointing from one end of the room to the other or by drawing one on the board. One end of the line is “Agree Very Much,” the mid-point is “Not Sure/Undecided,” and the other end of the line is “Disagree Very Much.”
- § Ask for five volunteers from the group. Tell them that they will serve as a “human graph.” Explain that you will ask them a series of statements and that they will react to each statement by standing in front of the part of the graph that corresponds to their opinion.
- § Instruct the class that the members of the human graph are not allowed to speak; therefore, the class will have to interpret their thoughts for them.
- § Select a few statements on Handout D, “Questions: National Security and Personal Privacy.” After each statement, allow time for the “human graph” to understand the statement and react by physically moving to a position on the line. Then ask the rest of the group to explain why they think the participants in the human graph are standing where they are. You may choose to let the human graph students explain their position after all of the students have commented.
- § The human graph students should feel free to move about on the line, changing their opinion if an argument seems persuasive to them. Continue with this process until all statements have been evaluated and discussed. Select additional groups of five for other questions.
- § Note: This activity can also be done with the entire group along the line. When the whole class is the graph, ask questions of different members about why they chose to stand where they stood.

Followup Questions

After the graph has finished representing the questions, students get into pairs. One student from each pair will identify the three biggest advantages of implementing the TIA project. The other student in the pair will identify the three biggest disadvantages of implementing the TIA project. Allow three minutes for each side to share their ideas.

Debrief as a large group using the following questions:

- § In your pair, what were the three strongest arguments in favor of the Total Information Awareness project? The three strongest arguments against?
- § What surprised you about the human graph? How did the participants in the graph shape your thinking about the Total Information Awareness project?

D: Questions: National Security and Personal Privacy

Questions for A Human Graph

- § In order to prevent future terrorist attacks against the United States, the federal government needs to do a better job of “connecting the dots” about terrorist activities here in the U.S.
- § When working to prevent terrorism, the federal government must still protect our rights as Americans. Otherwise, the terrorists will have won.
- § To help “connect the dots,” it is reasonable that the federal government should be able to combine information it already has about people in its existing databases into one big database.
- § A single federal database of personal information goes against our system of checks and balances in government.
- § Innocent people do not have to worry about the federal government keeping track of their personal information.
- § A reasonable balance between national security and personal privacy would provide the federal government access to:
 - Financial Records
 - Internet/email use
 - Library/Video Records
 - Medical Records
 - School Records
 - Travel Histories
- § Having the federal government keep track of personal data seems like an effective way to prevent future terrorist attacks.
- § The government is very effective at keeping information secure and safe.

E: Activity: Developing Total Information Awareness: A Presidential Commission

In a democracy, you have a say on government policies. This simulation is designed to help students understand how policies work and to provide them with a tool for assessing them.

Instructions

Divide students into groups of three or four.

Tell students to imagine that they are members of a commission appointed by the president to make a recommendation on whether to develop the Total Information Awareness project. Explain that their commission has been provided with the information featured in the reading A, "What is Total Information Awareness?"

To help them with their task, have them evaluate the policy using Handout F, "G R A D E." Briefly review the GRADE instrument and how it works.

Have each group assign roles: a commission chairperson (who leads the discussion), a recorder (who writes the group's answers to each GRADE test on a sheet of paper), a reporter (who reports the commission's findings to the class), and, if the group has four members, a responder (who answers any questions the class may have about the group's findings).

When the groups finish, ask them to indicate which recommendation they offered. Call on reporters from the groups in favor of developing Total Information Awareness to answer different GRADE tests. Then call on reporters from groups opposing development of Total Information Awareness to answer the GRADE tests.

When all groups have reported, ask the class as a whole to vote on whether or not to develop the project.

Followup Questions

- § Was your group for or against developing Total Information Awareness? What part of GRADE – Goal, Rivals, Advantages, Disadvantages, Evaluation – was most useful?
- § Did you change your position during the group reports? If so, what did you find most persuasive?
- § Did you decide differently than your group? If so, did working with your group help you understand their position?

F: Strategy: Looking at Public Policy: G R A D E

Public Policy is a plan of action, adopted by government, to solve a problem or reach a goal.”

In a democracy, you have a say on government policies and proposed policies. It's important that you take a critical look at them. Use the following GRADE test to analyze the Total Information Awareness project.

Goal	What is the policy and what is its goal? If you don't know what it's supposed to do, you can't measure its success or failure. Policies are designed to address problems. What problem or problems is this policy supposed to address?
Rivals	Who supports this policy? Who opposes it? Knowing the rivals can help you understand who the policy might affect and whether the policy favors special interest. Also, rivals are terrific sources for information. Be sure to check their facts though.
Advantages	What are the policy's benefits? What is good about the policy? Will it achieve (or has it achieved) its goal? Will it achieve the goal efficiently? Is it inexpensive? Does it protect people from harm? Does it ensure people's liberties?
Disadvantages	What are the policy's costs? What is bad about the policy? Is it inefficient? Is it expensive? Does it cause harm? Does it intrude on people's liberties? Are there any potential consequences that may cause damage?
Evaluate the alternatives	One alternative is to do nothing. Most serious problems have various policy proposals. Evaluate them. Look at their goals, advantages, and disadvantages.

Adapted from: The Challenge of Information, © 1998, Constitutional Rights Foundation (Los Angeles)

Taking a Stand: Position Paper on Total Information Awareness

Policy

Should the U.S. Government develop the Total Information Awareness project?

Steps for Writing Your Position Paper

1. Choose a position for, against, or as an alternative to the policy above.
2. Then team up with classmates who take the same position and as a group, write a persuasive paper arguing the benefits associated with your position on this policy.
3. In your essay, be sure to call on the most convincing arguments and specific evidence and examples from:
 - § the reading
 - § discussion and other classroom activities
 - § people in your community
 - § any other sources available to you
4. Include in your paper the most convincing arguments from the opposing side. List what you think are the best arguments your policy rivals would make. Acknowledge these points, and do your best to refute the importance of these details.

Specifications for Your Paper

Length. Your paper should be between 300 and 500 words.

Format. Each paper must have the name of the school in the heading and the policy being addressed in the title. No student names will appear on the position papers.

Sharing Your Views

Send your position paper to your U.S. Representative and/or U.S. Senators in Congress. You can find their address through <http://Thomas.loc.gov>.

Creating a Federal Database: Selected Community, Print, and Internet Resources

Resources

American Civil Liberties Union of Illinois
180 North Michigan Avenue #2300
Chicago, Illinois 60601-1287
312/201-9740
<http://www.aclu-il.org/>

Defense Advanced Research Projects Agency
United States Department of Defense
571/248-1532
<http://www.darpa.mil/>

Electronic Frontier Foundation
www.eff.org

Electronic Privacy Information Center
1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009
202/483-1140
<http://www.epic.org>

Illinois Secretary of State Jesse White
<http://www.sos.state.il.us/>

Information Awareness Office, Defense Advanced Research Projects Agency
<http://www.darpa.mil/iao/>

Institute for Defense Analyses
<http://www.ida.org/>

Office of the U.S. Attorney, Northern District of Illinois
219 South Dearborn Street, 4th floor
Chicago, IL 60604
312/353-5300
<http://www.usdoj.gov/usao/iln/>

Public Inquiry Office
United States Department of Defense
703/428-0711

Documents

Total Information Awareness (TIA) System
Information Awareness Office, Defense Advanced Research Projects Agency
<http://www.darpa.mil/iao/TIASystems.htm>

Defense Advanced Research Projects Agency's Information Awareness Office and Total Information Awareness Project
<http://www.arpa.mil/iao/iaotia.pdf>

Information and Analysis

Anderson, Curt. "U.S. Wants to Track Foreign Travelers' Comings and Goings; Americans would Have to Detail Trips." Associated Press January 4, 2003.

Atlantic Online. "Technology and Security." The Atlantic.Com. August, 21, 2002
<http://www.theatlantic.com/cgi-bin>.

Bovt, Georgi. "Hello, Big Brother," *Isvestiya*, November 26, 2002 :Vol. 50, No. 2.

Brune, Tom. "Pentagon Refutes 'Big Brother' Charge." *Newsday.com* November 21, 2002
<http://www.newsday.com/news/nationworld/nation/ny-uspeek1121,0,348253.story>.

Clymer, Adam. "Senate Votes to Curb Project to Search for Terrorists in Databases and Internet Mail." *New York Times* January 24, 2003
<http://www.nytimes.com/2003/01/24/national/24PRIV.html?ex=1044689273&ei=1&en=104edeafd3c781f2>.

Costello, Mark; Michael Moynihan, Ron Sege, Colin Westin, and Alan Harrison. "The Searchable Soul: Privacy in the Age of Information Technology (Forum)." *Harper's Magazine* January 2000, pp. 57-68.

Electronic Privacy Information Center. "Total Information Awareness."
<http://www.epic.org/privacy/profiling/tia/>

Garamone, Jim. "Rumsfeld Says Don't Sweat DARPA Info Awareness Experiment." *American Forces Press Service* November 2002
http://www.defenselink.mil/news/Nov2002/n11182002_200211181.html.

Harris, Shane. "Tech Insider: Total Information Unawareness." *Government Executive.com* November 20, 2002
<http://www.covexec.com/nes.index.cfm?mode=reprot&articleid=24525>.

Healy, Gene. "Beware of Total Information Awareness." *Cato Institute* January 20, 2003
<http://www.cato.org/dailys/01-20-03.html>.

Institute for Defense Analyses. "Security with Privacy." *Information Science and Technology (ISAT) study group* December 13, 2002
<http://www.arpa.mil/iao/secpriv.pdf>.

Markoff, John and John Schwartz. "Many Tools of Big Brother Are Up and Running." *The New York Times* December 23, 2002
<http://www.nytimes.com/2002/23/technology>.

Milstein, Sarah. "Taming the Task of Checking for Terrorists' Names." *The New York Times* December 30, 2002.

Simpson, Cam. "Homeland Bill Offers No Funds to Fix Computer Incompatibility." *Chicago Tribune* January 5, 2003.

Singel, Ryan. "Total Info System Totally Touchy," *Wired*, December 2, 2002
<http://www.wired.com/news/politics/0,1283,56620,00.html>.

Stanley, Jay and Barry Steinhardt. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society." January 2003: *American Civil Liberties Union, Technology and Liberty Program* <<http://www.aclu.org/Privacy/Privacylist.cfm?c=39>>.

United States Department of Defense. "DoD News Briefing-ASD(PA) Clarke and Adm.Gove." *News Transcript* November 20, 2002
http://www.defenselink.mil/news/Nov2002/t11202002_t1120asd.html.