Bill as Introduced

HCR 9 – AS INTRODUCED

2003 SESSION

03-0710
05/09

HOUSE CONCURRENT RESOLUTION *9*

A RESOLUTION urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

SPONSORS: Rep. Almy, Graf 18; Rep. Kurk, Hills 48; Rep. M. Smith, Straf 72; Rep. Buhlman, Hills 66

COMMITTEE: State-Federal Relations and Veterans Affairs

ANALYSIS

This resolution urges the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

HCR 9 – AS INTRODUCED

03-0710
05/09

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Three

A RESOLUTION urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

Whereas, our nation and our state were founded to escape and prevent tyranny by the establishment of multiple checks upon the power of our respective governments, and by the careful restraint of our military's power over our civilian population; and

Whereas, the Department of Defense of the United States of America is now exploring a program named Total Information Awareness which would attempt to requisition and correlate every existing private and public database on our nation's individual citizens and residents; and

Whereas, these databases are said to include those of credit records, employment histories, gun registries, medical records, educational records, drivers' licenses, catalog purchases, civil lawsuits, criminal proceedings, Social Security information, professional licenses, passport applications, civil and military service dossiers, bank accounts, computerized road toll records, IRS records, insurance records, savings and debt transactions, airline travel, FBI and police dossiers, video and cable viewing records, surveillance cameras, computer activity records, and library records; and

Whereas, this degree of government knowledge of the lives of ordinary Americans, and potential control of their individual data, could be devastating to our liberty and our republic, if ever used for personal or political gain by individual government employees, or by a future commander in chief or agency head for control of legitimate domestic dissent, political activity, key economic actors, or the media; and

Whereas, even under the assumption that no future office-holder would be tempted by the illegitimate abuse of this vast power over the citizenry, the temptation to extend its use into the civilian concerns of ordinary crime would be difficult to resist and effectively abolish all constitutional guarantees against government searches and seizures; now, therefore, be it

Resolved by the House of Representatives, the Senate concurring:

That the Commander in Chief and the Joint Chiefs of Staff of the United States of America are strongly urged to abandon the attempt to implement the Total Information Awareness program; and

That copies of this resolution be forwarded by the house clerk to each member of the New Hampshire congressional delegation, the President of the United States, and the Joint Chiefs of Staff in Arlington, Virginia.

Speakers

SIGN UP SHEET

To Register Opinion If Not Speaking

Bill # HCR 9 Date 2/4/03

Committee JF

** Please Print All Information **

Name	Address	Phone	Representing	(check one) Pro	Con
Rep J P Manning			28	✓	
Jerome Holden	P.O. Box 1085	Wilkesboro	5695735	GeHB ✓	
James Pollock				✓	
Rep Barbara Hunt Rutherford		Christie 26		✓	

Hearing Minutes

HOUSE COMMITTEE ON STATE-FEDERAL RELATIONS AND VETERANS AFFAIRS

PUBLIC HEARING ON HCR 9

BILL TITLE: urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

DATE: February 04, 2003

LOB ROOM: 306 **Time Public Hearing Called to Order:** 11:00am

Time Adjourned: 11:45am

(please circle if present)

Committee Members: Reps. Coughlin, Guay, D. Fields, Priestley, Albert, Balcom, Lessard, Marple, Easson, Hawkins, Headd, Kenney, Kerns, McCann, McElroy, McDonough-Wallace, Heon, Batchelder, Shaw, P. Sullivan and Sweeney.

Bill Sponsors: Rep. Almy, Rep. kurk, Rep. M Smith, Rep. Buhlman

TESTIMONY

* Use asterisk if written testimony and/or amendments are submitted.

* **Rep. Almy, prime sponsor**, spoke in support and provided written testimony. She stated that this was a "new start" program to link all citizens to terrorists dealing with surveillance. She stated that this is not a path that this country should follow.

Rep. Marple questioned if this was a violation of the 4th Amendment. Rep. Almy responded by stating that she was not aware of this invasion of tyranny.

Rep. Sullivan asked if a search warrant would be necessary. Rep. Almy responded by stating that it would be impossible to get all search warrants.

* **Rep. Smith, co-sponsor**, submitted written testimony. She stated that it was Mr. Poindexter's intent to find information on every citizen, where you eat, and with whom, medical records, all information collected, could be collected. This opens up personal information. We know our values as Americans.

Rep. Kurk, co-sponsor, spoke in support of this legislation. He stated that the problem with TIA assumes that every American is guilty. This is unacceptable to Americans. Hoover took advantage to put pressure. President Nixon compiled information to use against America improperly. Some will abuse power. This is the wrong way to go in times of war and terrorists. This is not a partisan issue. He strongly urged the committee to support this legislation.

Rep. Albert asked Rep. Kurk if the US Senate supports this issue. Rep. Kurk responded in the affirmative.

Rep. McElroy asked if this was part of the homeland security. Rep. Kurk responded by stating that this would change individual's way of life. We need to defend ourselves by the courts as we have always done. Not violate our rights to due process.

Wiltrud R. Mott-Smith supports this legislation but did not speak.

Respectfully submitted,

Dennis H. Fields, Clerk

Testimony

Excerpts of testimony on HCR 9, urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative, delivered before the State Federal Relations and Veterans Affairs Committee by Representative Marjorie K. Smith, Strafford 72, on February 4, 2003

Mr. Chairman, I support HCR 9 and urge you to consider that the United States Senate shares our concern about serious threats to the civil liberties that TIA poses to law abiding citizens. On this issue, at this time, a resolution from the state of New Hampshire could help to influence the final outcome.

On January 23, the United States Senate accepted an amendment to a spending bill that will suspend the development of the Total Information Awareness (TIA) system. Funding for development of TIA will end 60 days after the passage of the bill unless the intelligence community submits a detailed report to Congress on the privacy and civil liberties implications of the system. The amendment further requires Congressional authorization before TIA is deployed by any agency. However, exceptions in the amendment allow President Bush to approve continued funding for TIA, and the use of TIA for military operations outside the United States.

Without congressional review and oversight, data-mining would allow the Department of Homeland Security, the Department of Defense and other government agencies to collect and analyze a combination of intelligence data and personal information, including an individual's traffic violations, credit card purchases, travel records, medical records, communications records including email, and virtually any information collected on commercial, public or private governmental databases.

Many members of the U.S. Senate and House of Representatives have expressed alarm. Senator Charles Grassley (R – IA) in a recent letter to Attorney General John Ashcroft expressed concern about TIA "being applied to U.S. citizens and its chilling impact on civil liberties." Senator Grassley asked the Attorney General to reconcile two statements, one in which the Justice Department said that it had not gotten any information about TIA and one in which representatives of the Department of Defense said it was their understanding that the FBI and the Department of Defense were working on a memorandum of understanding with reference to TIA. He concluded, "I am very concerned that DoJ and the FBI may have been less than forthright to the press and the American people about their involvement with TIA."

I am attaching copies of the Senate Amendment and several articles which detail the legitimate concerns felt by many about this attack on the civil liberties of law abiding citizens.

ATTACHMENTS:

U.S. Senate Amendment 59 to H.J. Res 2, January 23, 2003
"Beware of Total Information Awareness" by Gene Healy, senior editor, Cato Institute
"Dick Armey's Warning" by Nat Hentoff, columnist, The Washington Times

MAKING FURTHER CONTINUING APPROPRIATIONS FOR FISCAL YEAR 2003 --
(Senate - January 23, 2003)

[Page: S1412]

[...]

AMENDMENT NO. 59
(Purpose: To provide certain limitations and prohibitions on the development and deployment of the Total Information Awareness program)

At the end of title I of division M, add the following:

[Page: S1413]

SEC. 111. (a) LIMITATION ON USE OF FUNDS FOR RESEARCH AND DEVELOPMENT ON TOTAL INFORMATION AWARENESS PROGRAM.--Notwithstanding any other provision of law, commencing 60 days after the date of the enactment of this Act, no funds appropriated or otherwise made available to the Department of Defense, whether to an element of the Defense Advanced Research Projects Agency or any other element, or to any other department, agency, or element of the Federal Government, may be obligated or expended on research and development on the Total Information Awareness program unless--

(1) the report described in subsection (b) is submitted to Congress not later than 60 days after the date of the enactment of this Act; or

(2) the President certifies to Congress in writing, that--

(A) the submittal of the report to Congress within 60 days after the date of the enactment of this Act is not practicable; and

(B) the cessation of research and development on the Total Information Awareness program would endanger the national security of the United States.

(b) REPORT.--The report described in this subsection is a report, in writing, of the Secretary of Defense, the Attorney General, and the Director of Central Intelligence, acting jointly, that--

(1) contains--

(A) a detailed explanation of the actual and intended use of funds for each project and activity of the Total Information Awareness program, including an expenditure plan for the use of such funds;

(B) the schedule for proposed research and development on each project and activity of the Total Information Awareness program; and

(C) target dates for the deployment of each project and activity of the Total Information Awareness program;

(2) assesses the likely efficacy of systems such as the Total Information Awareness program in providing practically valuable predictive assessments of the plans, intentions, or capabilities of terrorists or terrorist groups;

(3) assesses the likely impact of the implementation of a system such as the Total Information Awareness program on privacy and civil liberties; and

(4) sets forth a list of the laws and regulations that govern the information to be collected by the Total Information Awareness program, and a description of any modifications of such laws that will be required to use the information in the manner proposed under such program;

(5) includes recommendations, endorsed by the Attorney General, for practices, procedures, regulations, or legislation on the deployment, implementation, or use of the Total Information Awareness program to eliminate or minimize adverse effects of such program on privacy and other civil liberties.

(c) LIMITATION ON DEPLOYMENT OF TOTAL INFORMATION AWARENESS PROGRAM.--(1) Notwithstanding

any other provision of law and except as provided in paragraph (2), if and when research and development on the Total Information Awareness program, or any component of such program, permits the deployment or implementation of such program or component, no department, agency, or element of the Federal Government may deploy or implement such program or component, or transfer such program or component to another department, agency, or element of the Federal Government, until the Secretary of Defense--

(A) notifies Congress of that development, including a specific and detailed description of--

(i) each element of such program or component intended to be deployed or implemented; and

(ii) the method and scope of the intended deployment or implementation of such program or component (including the data or information to be accessed or used); and

(B) has received specific authorization by law from Congress for the deployment or implementation of such program or component, including--

(i) a specific authorization by law for the deployment or implementation of such program or component; and

(ii) a specific appropriation by law of funds for the deployment or implementation of such program or component.

(2) The limitation in paragraph (1) shall not apply with respect to the deployment or implementation of the Total Information Awareness program, or a component of such program, in support of the following:

(A) Lawful military operations of the United States conducted outside the United States.

(B) Lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States persons.

(d) SENSE OF CONGRESS.--It is the sense of Congress that--

(1) the Total Information Awareness program should not be used to develop technologies for use in conducting intelligence activities or law enforcement activities against United States persons without appropriate consultation with Congress or without clear adherence to principles to protect civil liberties and privacy; and

(2) the primary purpose of the Defense Advanced Research Projects Agency is to support the lawful activities of the Department of Defense and the national security programs conducted pursuant to the laws assembled for codification purposes in title 50, United States Code.

(e) DEFINITIONS.--In this section:

(1) TOTAL INFORMATION AWARENESS PROGRAM.--The term ``Total Information Awareness program''--

(A) means the computer hardware and software components of the program known as Total Information Awareness, any related information awareness program, or any successor program under the Defense Advanced Research Projects Agency or another element of the Department of Defense; and

(B) includes a program referred to in subparagraph (1), or a component of such program, that has been transferred from the Defense Advanced Research Projects Agency or another element of the Department of Defense to any other department, agency, or element of the Federal Government.

(2) NON-UNITED STATES PERSON.--The term ``non-United States person'' means any person other than a United States person.

(3) UNITED STATES PERSON.--The term ``United States person'' has the meaning given that term in section 101(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(i)).

Beware of Total Information Awareness

by Gene Healy

Gene Healy is senior editor at the Cato Institute.

John Poindexter, head of the Pentagon's Office of Information Awareness, is developing a vast surveillance database to track terror suspects. The Total Information Awareness (TIA) system will, according to Poindexter, "break down the stovepipes" that separate commercial and government databases, allowing OIA access to citizens' credit card purchases, travel itineraries, telephone calling records, email, medical histories and financial information. It would give government the power to generate a comprehensive data profile on any U.S. citizen.

Adm. Poindexter assures us that TIA will be designed to respect constitutional guarantees of privacy and shield law-abiding citizens from the Pentagon's all-seeing eye. But if the history of military surveillance of civilians is any indication, accepting that assurance amounts to the triumph of hope over experience.

Opponents of new government surveillance measures such as TIA or Operation TIPS, the Justice Department's aborted plan to utilize citizen informants, often invoke the specter of the East German secret police and communist Cuba's block watch system. But we don't have to look to totalitarian states for cautionary tales. There's a long and troubling history of military surveillance in this country. That history suggests that we should loathe allowing the Pentagon access to our personal information.

During World War I, concerns about German saboteurs led to unrestrained domestic spying by U.S. Army intelligence operatives. Army spies were given free reign to gather information on potential subversives, and were often empowered to make arrests as special police officers. Occasionally, they carried false identification as employees of public utilities to allow them, as the chief intelligence officer for the Western Department put it, "to enter offices or residences of suspects gracefully, and thereby obtain data." In her book "Army Surveillance in America," historian Joan M. Jensen notes, "What began as a system to protect the government from enemy agents became a vast surveillance system to watch civilians who violated no law but who objected to wartime policies or to the war itself."

The War Department relied heavily on a quasi-private volunteer organization, the American Protective League, composed of self-styled patriots who agreed to inform on their fellow citizens. America's experience with the APL makes clear that civil libertarian concerns about Operation TIPS are, if anything, understated. APL volunteers carried identification cards and tin badges and responded to requests from the War Department for investigation of civilians. By the end of the war the APL had close to a quarter of a million members and had carried out some six million investigations.

At the War Department's request, APL volunteers harassed labor organizers, intimidated and arrested opponents of the draft, and investigated such potential subversives as Mexican-American leaders in Los Angeles, pacifist groups, and antiwar religious sects. Through it all, the army caught exactly one German spy, a naval officer who tried to enter the United States via Nogales, Arizona.

The Army's domestic surveillance activities were substantially curtailed after the end of World War I. But throughout the 20th Century, in periods of domestic unrest and foreign conflict, army surveillance ratcheted up again, most notably in the 1960s. During that tumultuous decade, President Johnson repeatedly called on federal troops to quell riots and restore order. To better perform that task, Army intelligence operatives began compiling thousands of dossiers on citizens, many of whom had committed no offense beyond protesting government policy. Reviewing the files, the Senate Judiciary Committee noted that "comments about the financial affairs, sex lives and psychiatric histories of persons unaffiliated with the armed forces appear throughout the various records systems." Justice William O. Douglas called army surveillance "a cancer in our body politic."

Adm. Poindexter seeks to bring Pentagon surveillance into the 21st Century, replacing the low-tech, labor intensive system relied on in the past with high-tech data-mining techniques. He maintains that "we can achieve the necessary security we need and still have privacy." But given the military's legacy of privacy abuses, such vague assurances are cold comfort.

Some have suggested that Poindexter's record as a former Iran-Contra defendant convicted of five felony counts of lying to Congress disqualify him from his position. But the question isn't whether Poindexter's the right man for the job; it's whether that job should exist in the first place

Dick Armey's warning

Nat Hentoff

During his years in Congress, Dick Armey was a firm and incisive defender of conservative values. Individual constitutional liberties against the government were very much among them. In his December 6 farewell address at the National Press Club, the retiring Republican Majority Leader warned of the "awful, dangerous seduction" of sacrificing our freedoms for safety in our war to defeat "this insidious threat that comes right into our neighborhood."

Armey emphasized that "we the people, had better keep an eye on ... our government. Not out of contempt or lack of appreciation or disrespect, but out of a sense of guardianship.

"How do you use these tools we have given you to make us safe in such a manner that'll preserve our freedom? ... Freedom is no policy for the timid. And my plaintive plea to all my colleagues that remain in this government as I leave it is, for your sake, for my sake, for heaven's sake, don't give up on freedom!"

Hearing Armey's speech, I was reminded of one of the last conversations I had with the late Supreme Court Justice William Brennan. He and Armey greatly disagreed on some issues, but not on certain essential sections of the Bill of Rights.

"Look, pal," Justice Brennan told me, "we've always known — the Framers knew — that liberty is a fragile thing."

The deepening concern about the unpredictable dangers, internal and external, of terrorism also extends to the creation by our government of what Charles Lane of the Washington Post accurately calls "a parallel legal system." That system has enlisted many conservatives to guard the Bill of Rights. I've been on some of these conservatives' radio programs to discuss the issue.

Former Republican Congressman Bob Barr of Georgia — speaking on CNN about the massive data-collecting Total Information Awareness (TIA) system being developed in Donald Rumsfeld's Pentagon — said that "millions of Americans will have their privacy invaded in ways they will never know."

An attempt by the Electronic Privacy Information Center (EPIC) to convince the Senate to stop the TIA dragnet failed. However, not only did the American Civil Liberties Union support EPIC's endeavor, but also Phyllis Schafly's Eagle Forum, the Free Congress Foundation and the American Library Association.

Armey and Barr are working with the ACLU on privacy and other civil liberties issues. Not surprisingly, some politically correct members of the ACLU are disturbed.

In a letter to the membership, Executive Director Anthony Romero reminded them that "throughout our 82-year-old history, we have aligned ourselves with people who can help us protect civil liberties regardless of their political party. ... The Civil Rights Act of 1991, signed into law by President George H.W. Bush, was the result of ... unlikely allies across the Democratic and Republican parties."

Romero adds that the ACLU "has no permanent friends and no permanent enemies, just permanent values." Illustrating that point is Illinois Republican Congressman Henry Hyde, who has often clashed with the ACLU. But he has worked with it to protect free speech on college campuses and to limit the right of government to seek defendants' assets in certain cases. "They

are," he says of the ACLU, "a very useful and productive force in jurisprudence."

As a pro-lifer, I have had profound disagreements with the ACLU, including its failure to support the free-speech rights of the pro-lifers in the current Supreme Court case Scheidler v. the National Organization for Women. This involves the ominous use of the harsh Racketeer Influence and Corrupt Organizations Act (RICO) penalties, normally used to battle corruption, to quell political or social protests. If upheld, this will affect diverse demonstrators both left and right.

But — as Armey and Barr have warned — the continuing invasions of basic liberties in the USA Patriot Act and the subsequent insistence by the administration to set up an additional parallel legal system, affects all of our freedoms. And the ACLU has proved essential in that battle.

Since Sept. 11, 2001, ACLU membership has swelled by 50,000 people, and the total number of dues payers is 350,000. For more and more Americans, it is no longer an epithet to refer to "card-carrying members of the ACLU." And more than 50,000 Americans are joining the rapidly growing number of the Bill of Rights Defense Committees in towns and cities across the country.

As Dick Armey says: "Don't give up on freedom!"

Nat Hentoff is a columnist for The Washington Times. His column runs on Mondays.

From: DBuhlman@aol.com
Date: Sat, 1 Feb 2003 15:26:59 EST
Subject: HCR9
To: susan.almy@valley.net

TO: The Honorable Members of the State Federal Relations and Veterans Affairs Committee

RE: Testimony in Support of HCR9

FROM: Representative David Buhlman, District 66, Hudson-Pelham

Due to other commitments it was not possible to appear today to express my strong support of HCR9. Following is my testimony:

The federal government's Total Information Awareness Initiative (TIAI) seeks to track and store information on all Americans in a central data base.

This is a chilling concept in the land of liberty. And the warrantless searches associated with this program are in clear violation of the Fourth Amendment to the Constitution of the United States.

The terrorists attacks on September 11th were sickening acts of depraved individuals. But the destruction they caused should not be increased by government actions that threaten our basic rights. If we allow the assaults on the Bill of Rights to proceed unopposed, shame on us.

The state of New Hampshire, with its Live Free or Die tradition, must speak up loudly and clearly against the implementation of TIAI and any other similar liberty-threatening schemes.

WHAT DO YOU CARE IF YOU HAVE NOTHING TO HIDE?

That question is meant to put those who oppose such programs on the defensive. But what's next? Should we allow the police to search our homes unannounced? Should we stopped and frisked on the streets without cause?

In America we do not have to prove to the government that we have nothing to hide. The Constitution says so, and if we allow the Constitution to be violated by the government in such a cavalier manner with TIAI, we have lost the Republic.

Please vote OTP on HCR9.

Thank you.

Representative David Buhlman, District 66, Hudson-Pelham

Date
NOV 14TH 2002

WILLIAM SAFIRE

You Are a Suspect

WASHINGTON

If the Homeland Security Act is not amended before passage, here is what will happen to you:

Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade your receive, every bank deposit you make, every trip you book and every event you attend — all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database."

To this computerized dossier on your private life from commercial sources, add every piece of information that government has about you — passport application, driver's license and bridge toll records, judicial and divorce records, complaints from nosy neighbors to the F.B.I., your lifetime paper trail plus the latest hidden camera surveillance — and you have the supersnoop's dream: a "Total Information Awareness" about every U.S. citizen.

This is not some far-out Orwellian scenario. It is what will happen to your personal freedom in the next few weeks if John Poindexter gets the unprecedented power he seeks.

Remember Poindexter? Brilliant man, first in his class at the Naval Academy, later earned a doctorate in physics, rose to national security adviser under President Ronald Reagan. He had this brilliant idea of secretly selling missiles to Iran to pay ransom for hostages, and with the illicit proceeds to illegally support contras in Nicaragua.

A jury convicted Poindexter in 1990 on five felony counts of misleading Congress and making false statements, but an appeals court overturned the verdict because Congress had given him immunity for his testimony. He famously asserted, "The buck stops here," arguing that the White House staff, and not the president, was responsible for fateful decisions that might prove embarrassing.

This ring-knocking master of deceit is back again with a plan even more scandalous than Iran-contra. He heads the "Information Awareness Office" in the otherwise excellent Defense Advanced Research Projects Agency, which spawned the Internet and stealth aircraft technology. Poindexter is now realizing his 20-year dream: getting the "data-mining" power to snoop on every public and private act of every American.

Even the hastily passed U.S.A. Patriot Act, which widened the scope of the Foreign Intelligence Surveillance Act and weakened 15 privacy laws, raised requirements for the government to report secret eavesdropping to Congress and the courts. But Poindexter's assault on individual privacy rides roughshod over such oversight.

He is determined to break down the wall between commercial snooping and secret government intrusion. The disgraced admiral dismisses such necessary differentiation as bureaucratic "stovepiping." And he has been given a $200 million budget to create computer dossiers on 300 million Americans.

When George W. Bush was running for president, he stood four-square in defense of each person's medical, financial and communications privacy. But Poindexter, whose contempt for the restraints of oversight drew the Reagan administration into its most serious blunder, is still operating on the presumption that on such a sweeping theft of privacy rights, the buck ends with him and not with the president.

This time, however, he has been seizing power in the open. In the past week John Markoff of The Times, followed by Robert O'Harrow of The Washington Post, have revealed the extent of Poindexter's operation, but editorialists have not grasped its undermining of the Freedom of Information Act.

Political awareness can overcome "Total Information Awareness," the combined force of commercial and government snooping. In a similar overreach, Attorney General Ashcroft tried his Terrorism Information and Prevention System (TIPS), but public outrage at the use of gossips and postal workers as snoops caused the House to shoot it down. The Senate should now do the same to this other exploitation of fear.

The Latin motto over Poindexter"s new Pentagon office reads "Scientia Est Potentia" — "knowledge is power." Exactly: the government's infinite knowledge about you is its power over you. "We're just as concerned as the next person with protecting privacy," this brilliant mind blandly assured The Post. A jury found he spoke falsely before. □

E-mail: safire@nytimes.com

Secu

The H
rity bil
that ne
and Re

Road

Arizona
Kansas
to eme
champi

ELECTRONIC PRIVACY INFORMATION CENTER

Total Information Awareness (TIA)

Introduction | News | Resources

Introduction

The Total Information Awareness project is part of the Defense Advanced Research Projects Agency's Information Awareness Office. The office is headed by Admiral (retired) John Poindexter who is responsible for conceiving the project. TIA purports to capture the "information signature" of people so that the government can track potential terrorists and criminals involved in "low-intensity/low-density" forms of warfare and crime. The goal is to track individuals through collecting as much information about them as possible and using computer algorithms and human analysis to detect potential activity.

The project calls for the development of "revolutionary technology for ultra-large all-source information repositories," which would contain information from multiple sources to create a "virtual, centralized, grand database." This database would be populated by transaction data contained in current databases such as financial records, medical records, communication records, and travel records as well as new sources of information. Also fed into the database would be intelligence data.

A key component of the TIA project is to develop data-mining or knowledge discovery tools that will sort through the massive amounts of information to find patterns and associations. TIA will also develop search tools such as Project Genoa, which Admiral Poindexter's former employer Syntek Technologies, assisted in developing. TIA aims to fund the development of more such tools and data-mining technology to help analysts understand and even "preempt" future action.

A further crucial component is the development of biometric technology to enable the identification and tracking of individuals. DARPA has already funded its "Human ID at a Distance" program, which aims to positively identify people from a distance through technologies such as face recognition or gait recognition. A nationwide identification system would be of great assistance to such a project by providing an easy means to track individuals across multiple information sources.

DARPA's Broad Agency Announcement 02-08 soliciting proposals from industry states that the initial plan is for a five year research project into these various technologies. The interim goal is to build "leave-behind prototypes with a limited number of proof-of-concept demonstrations in extremely high risk, high payoff areas." The FBI and the Transportation Security Administration are also working on data-mining projects that will fuse commercial databases, public databases, and intelligence data and had meetings with TIA developers.

Search

Advanced Search
Help

Publications

- Books
- Policy Studies
- Cato Policy Report
- Cato Journal
- Regulation Magazine
- Cato Handbook for Congress
- Congressional Testimony
- Legal Briefs
- Cato Audio
- Cato's Letters
- To Be Governed...
- Events Archive

25th Anniversary

- 25th Home
- Friedman Prize
- Milton Friedman
- About Cato
- Cato Timeline

Contribute

- Make a Contribution
- About Sponsorship
- Alternative Giving Methods
- Levels and Benefits

Cato Online

December 7, 2002

Total Information Awareness: Back to the Future

by Charles V. Peña

Charles V. Peña is senior defense policy analyst at the Cato Institute.

The idea of "total information awareness," or TIA, has come under fire lately. And for good reason. This new system for intelligence gathering could backfire and lead to a repetition of the intelligence failures America experienced prior to 9/11.

TIA is a Pentagon program designed to build a large-scale counter-terrorism database from myriad sources, including e-mail, electronic and credit card purchases, airline travel, rental cars, telephone calling cards, gun purchases, and medical records.

Supporters argue that it's an advanced computer tool intended to help catch would-be terrorists by looking for links and patterns indicative of terrorist activity. Critics are concerned that the TIA program would be the first step towards a surveillance state and allow the U.S. government to monitor and spy on its own citizens. For example, some critics have written the following:

- "[W]e do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant government the Orwellian capability to listen at will and in real time to our communications across the Web?"

- "The administration's interest in e-mail is a wholly unhealthy precedent, especially given this administration's track record on FBI files and IRS snooping. Every medium by which people communicate can be subject to exploitation by those with illegal intentions. Nevertheless, this is no reason to hand Big Brother the keys to unlock our e-mail diaries, open our ATM records, read our medical records, or translate our international communications."

You would think such "alarmist" rhetoric is coming from groups such as the American Civil Liberties Union, the Electronic Privacy Information Center, or the Southeastern Legal Foundation -- all of whom have been critical of TIA.

You would be wrong.

January 2, 2003

Daily Commentary

Interventionism, Allegedly a Middle-of-the-Road Policy

by Ludwig von Mises

[Archives]

Daily Dispatch

- South Korea and China Act Diplomatically with North Korea
- D.C. Cuts Literacy Program
- New Study Says Global Warming is Forcing Many Species to Migrate

[Archives]

Pocket Constitution
Email Updates
Cato Audio
Cato Store

Those words were written in October 1997 by then-Senator John Ashcroft. He was taking issue with the Clinton administration's views on the Internet and proposed regulations and controls. Curiously, today, Attorney General Ashcroft has been deafeningly silent on the issue of TIA. Apparently, what's not good for the goose is okay for the gander.

But Ashcroft's concerns about the future of the Internet then are as valid when it comes to TIA now. Americans should not blindly give in to fear and a sense of vulnerability by giving the federal government (in particular, the executive branch) ever-expansive powers all in the name of homeland security and fighting the war on terrorism. The fundamental question is not whether TIA is a good idea right now because we must cope with a new terrorist threat. The question is whether TIA is a good idea, period -- whether in this, the previous, or successive administrations.

Concerns about TIA are threefold.

First and foremost is the issue of civil liberties. If government had a pristine record and this was the first and only proposal that potentially threatens civil liberties, perhaps the cause for concern might be less. But TIA is being proposed by an administration with a penchant for secrecy and a "trust us, we know what we're doing" attitude. This same administration also gave us the USA PATRIOT Act, which gives the executive branch extraordinary power absent judicial checks and balances. And even though it was explicitly prohibited in the Homeland Security Act, the administration had previously proposed the TIPS (Terrorist Information and Prevention System), which would have made us a nation of snitches.

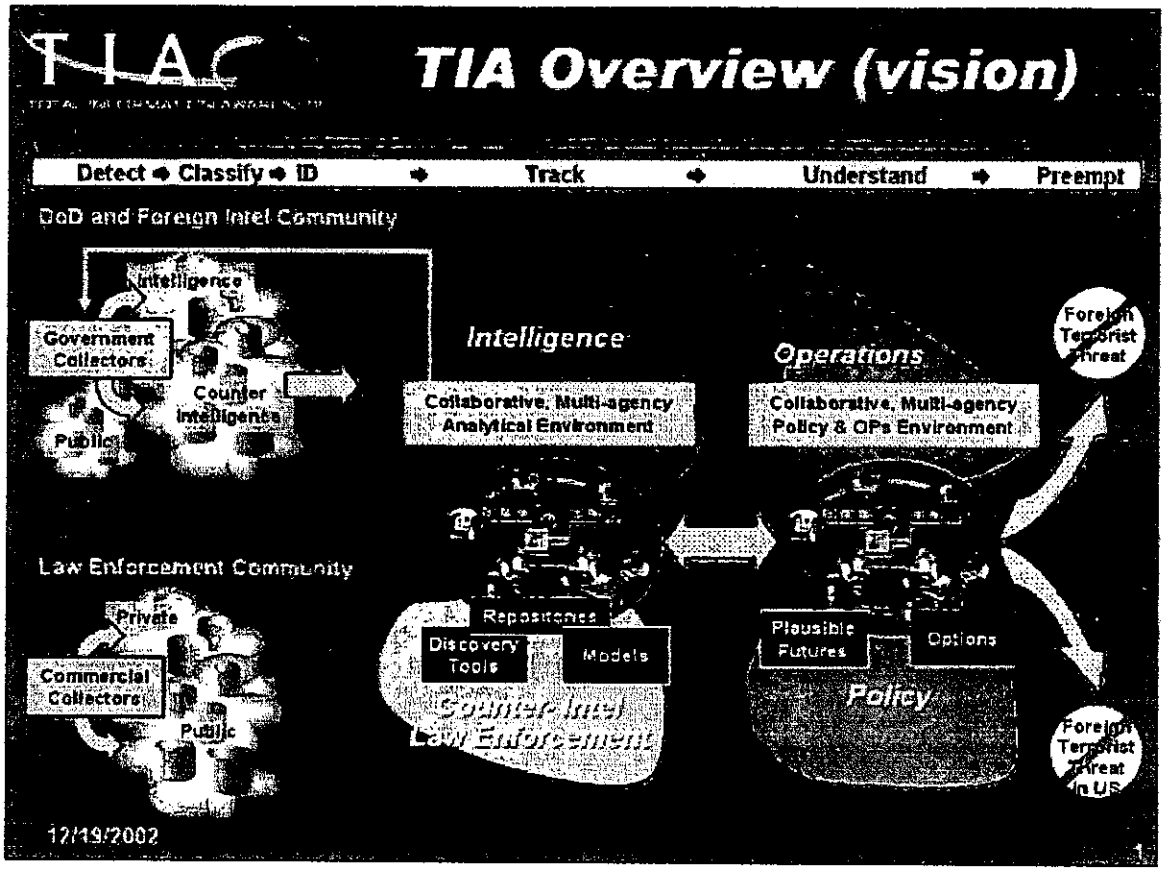
Second, how might TIA affect the information economy and electronic commerce? TIA is built on the premise of having access to transactional and record-keeping data. But people need to know that private information handed over to Internet service providers, banks, airlines, hotels, and other businesses will not routinely be given to the government and stored in a centralized database that -- despite cybersecurity -- could be hacked.

Third, how effective would TIA be in identifying and catching terrorists? TIA assumes that terrorists act according to certain patterns. If terrorist activity is static and unchanging, then the past could be predictive of the future. But the nature of terrorists is that they morph and adapt -- so they will likely learn the cues and patterns TIA is looking for and then avoid them. And this would increase the likelihood that TIA will mistakenly identify ordinary people as terrorists.

One final caution about TIA: It's being touted as a solution

Total Information Awareness: Back to the Future http://www.cato.org/dailys/12-07-02.html
to "connecting the dots" of intelligence data that weren't connected prior to Sept. 11. But another major intelligence shortcoming was over-reliance on technology and not enough human intelligence. The U.S. government needs to be careful about going back to the future with TIA and falling into the same trap.

Total Information Awareness (TIA) System



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.

Planned Accomplishments:

- TBA

Home News Programs Solicitations

Voting Sheets

HOUSE COMMITTEE ON STATE-FEDERAL RELATIONS AND VETERANS AFFAIRS

EXECUTIVE SESSION on HCR 9

BILL TITLE: **urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.**

DATE: March 06, 2003

LOB ROOM: 306

Amendments:

Sponsor: Rep. OLS Document #:

Sponsor: Rep. OLS Document #:

Sponsor: Rep. OLS Document #:

Motions: OTP, OTP/A, ITL, Interim Study (Please circle one.)

Moved by Rep. Hawkins

Seconded by Rep. Fields

Vote: 6-9 (Please attach record of roll call vote.)

Motions: OTP, OTP/A, ITL, Interim Study (Please circle one.)

Moved by Rep. Heon

Seconded by Rep. Sweeney

Vote: 14-1 (Please attach record of roll call vote.)

CONSENT CALENDAR VOTE: 15-0

(Vote to place on Consent Calendar must be unanimous.)

Statement of Intent: Refer to Committee Report

Respectfully submitted,

Rep. Dennis H. Fields, Clerk

HOUSE COMMITTEE ON STATE-FEDERAL RELATIONS AND VETERANS AFFAIRS

EXECUTIVE SESSION on HCR=9 3/6/2003

BILL TITLE: HCR=9

DATE: 3/6/2003

LOB ROOM: 306

Amendments:

Sponsor: Rep. _____ OLS Document #: _____ Adopted/Failed

Sponsor: Rep. _____ OLS Document #: _____ Adopted/Failed

Sponsor: Rep. _____ OLS Document #: _____ Adopted/Failed

Motions: OTP, OTP/A, (ITL), Interim Study (Please circle one.)

Moved by Rep. Hawkins

Seconded by Rep. FIELDS

Vote: 6 yeas, 9 nays (Please attach record of roll call vote.)

Motions: (OTP), OTP/A, ITL, Interim Study (Please circle one.)

Moved by Rep. Bean

Seconded by Rep. Sweeney

Vote: 14-1 (Please attach record of roll call vote.)

CONSENT CALENDAR VOTE: 15-0

(Vote to place on Consent Calendar must be unanimous.)

Statement of Intent: Refer to Committee Report

Respectfully submitted,

Rep. Dawn M. Fuller, Clerk

OFFICE OF THE HOUSE CLERK 2003 SESSION

STATE-FEDERAL RELATIONS AND VETERANS AFFAIRS

Bill #: HCR=9 Title: _____

PH Date: 2/04/2003 Exec Session Date: 3/06/2003

Motion: ITL Amendment #: _____

MEMBER	YEAS	NAYS
Coughlin, Pamela D. Chairman		
Guay, Lawrence J. V Chairman	/	
Fields, Dennis H	/	
Priestley, Anne K	/	
Albert, Russell A	/	
Balcom, John L	ABSENT.	
Lessard, Rudy	ABSENT	
Marple, Richard		/
Easson, Timothy E		/
Hawkins, Ken	/	
Headd, James F		/
Kenney, Bettie D		/
Kerns, J Edward	ABSENT.	
McCann, Richard A		/
McElroy, Henry W	/	
Heon, Richard F		/
McDonough-Wallace, Alice T	ABSENT.	
Shaw, Barbara E	ABSENT	
Sweeney, Cynthia P		/
Sullivan, Peter M		/
Batchelder, Robert C		/
	6	9

TOTAL VOTE:
Printed: 1/6/2003

OFFICE OF THE HOUSE CLERK 2003 SESSION

STATE-FEDERAL RELATIONS AND VETERANS AFFAIRS

Bill #: HCR-9 Title: _____

PH Date: 2/04/2003 Exec Session Date: 3/06/2003

Motion: OTP Amendment #: _____

MEMBER	YEAS	NAYS
Coughlin, Pamela D. Chairman		
Guay, Lawrence J. V Chairman	/	
Fields, Dennis H	/	
Priestley, Anne K	/	
Albert, Russell A	/	
Balcom, John L	ABSENT	
Lessard, Rudy	ABSENT	
Marple, Richard	/	
Easson, Timothy E	/	
Hawkins, Ken		/
Headd, James F	/	
Kenney, Bettie D	/	
Kerns, J Edward	ABSENT	
McCann, Richard A	/	
McElroy, Henry W	/	
Heon, Richard F	/	
McDonough-Wallace, Alice T		
Shaw, Barbara E		
Sweeney, Cynthia P	/	
Sullivan, Peter M	/	
Batchelder, Robert C	/	
	14	1

TOTAL VOTE:
Printed: 1/6/2003

Committee Report

COMMITTEE REPORT

COMMITTEE: **State-Federal Relations and Veterans Affairs**

BILL NUMBER: **HCR 9**

TITLE: urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

DATE: March 06, 2003 CONSENT CALENDAR YES ☒ NO ☐

☒ OUGHT TO PASS

☐ OUGHT TO PASS WITH AMENDMENT

☐ INEXPEDIENT TO LEGISLATE

☐ REFER TO COMMITTEE FOR INTERIM STUDY
(Available only in second year of biennium.)

STATEMENT OF INTENT
(Include Committee Vote)

This resolution urges the President and Joint Chiefs of Staff to abandon the Total Information Awareness Initiative (TIA). The federal government's TIA seeks to track and store information on all American in a central database. The committee felt that this degree of government knowledge of the lives of ordinary Americans could be devastating to our liberty and our republic. The committee feels that this resolution is important and necessary to protect the people of the State of New Hampshire.

Vote 14-1.

Rep. Richard F. Heon
FOR THE COMMITTEE

Original: House Clerk
cc: Committee Bill file

USE ANOTHER REPORT FOR MINORITY REPORT

CONSENT CALENDAR

State-Federal Relations and Veterans Affairs

HCR 9, urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative. **OUGHT TO PASS**

Rep. Richard F. Heon for State-Federal Relations and Veterans Affairs: This resolution urges the President and Joint Chiefs of Staff to abandon the Total Information Awareness Initiative (TIA). The federal government's TIA seeks to track and store information on all American in a central database. The committee felt that this degree of government knowledge of the lives of ordinary Americans could be devastating to our liberty and our republic. The committee feels that this resolution is important and necessary to protect the people of the State of New Hampshire. **Vote 14-1.**

COMMITTEE REPORT

COMMITTEE: STATE - Federal Relations Public Affairs

BILL NUMBER: HCR 9

TITLE: _____

_____

DATE: 3/06/2003 CONSENT CALENDAR: YES ☑ NO ☐

☒ OUGHT TO PASS

☐ OUGHT TO PASS W/ AMENDMENT

☐ INEXPEDIENT TO LEGISLATE

☐ RE-REFER

☐ INTERIM STUDY (Available only 2nd year of biennium)

Amendment No. _____

STATEMENT OF INTENT:

This Resolution urges the President and Joint Chiefs of Staff To Abandon the TOTAL Information Awareness Initiative. (TIA) The federal government's TIA seeks To Track and store information on all Americans in a central data base. The ~~Strong by partisan vote of the~~ committee felt that this degree of government knowledge of the lives of ordinary Americans could be devastating To our liberty and our Republic. The committee feels that this Resolution is important and

COMMITTEE VOTE: 14 - 1 (over)

- Copy to Committee Bill File
- Use Another Report for Minority Report

RESPECTFULLY SUBMITTED,

Rep. Richard J. Hess
For the Committee

Rev. 07/30/99

necessary To protect the people of the State of New Hampshire.