

The following is mirrored from its source at: <http://www.aclu.org/Privacy/Privacylist.cfm?c=130>

## Q&A on the Pentagon's "Total Information Awareness" Program

ACLU Technology and Liberty Program

January 2003



*TIA Logo -- The much-discussed original and the new, less frightening "sanitized" version.*

### What is the Total Information Awareness (TIA) Program?

TIA may be the closest thing to a true "Big Brother" program that has ever been seriously contemplated in the United States. It is based on a vision of pulling together as much information as possible about as many people as possible into an "ultra-large-scale" database, making that information available to government officials, and sorting through it to try to identify terrorists. Since the amount of public and private information on our lives is growing by leaps and bounds every week, a government project that seeks to put all that information together is a radical and frightening thing.

### Who runs the program?

TIA is run by the Defense Advanced Research Projects Agency (DARPA), a branch of the Department of Defense that works on military research. It is headed by John Poindexter, the former Reagan-era National Security Adviser known for his involvement in the Iran-Contra scandal, who famously said that it was his duty to withhold information from Congress.

### Is this program unique?

No. There is another effort underway that could bring about a similar result: an airline

profiling system called CAPS II. CAPS II would collect massive amounts of information about the tens of millions of American who fly each year and use that information to create profiles. Its use in the airline context gives it a lot more surface appeal, and it has been presented in a far less threatening manner, but it is based on the same faulty premise that terrorism can be prevented by collecting hoards of information about everyone and then subjecting them to a virtual dragnet.

### **How much information would be available to the program?**

Virtual dragnet programs like TIA and CAPS II are based on the premise that the best way to protect America against terrorism is to for the government to collect as much information as it can about everyone - and these days, that is a LOT of information. They could incorporate not only government records of all kinds but individuals' medical and financial records, political beliefs, travel history, prescriptions, buying habits, communications (phone calls, e-mails and Web surfing), school records, personal and family associations, and so on.

In the last decade we have witnessed an enormous explosion in the amount of tracking and information of individuals in the United States, due mainly to two factors:

- **Technology.** The explosion of computers, cameras, location-sensors, wireless communication, biometrics, and other technologies is making it a lot easier to track, store, and analyze information about individuals' activities.
- **The commercialization of data.** Corporations in recent years have discovered that detailed information about consumers is extremely valuable, and are in the process of figuring out how to squeeze every available penny out of this revenue source. That is why consumers are increasingly being asked for their information everywhere they turn, from product registration forms to loyalty programs to sweepstakes entry forms. As a result, private sector incentives are now aligned with the interests of those in government who wish to track everyone's behavior. The government has not been shy about buying that data, and it is envisioned as a primary source for the TIA database.

The information that is generated and retained about our activities is becoming so rich that if all that information about us was put together, it would almost be like having a video camera following us around. Programs like TIA would make such "data surveillance" a reality.

### **What is wrong with the TIA Program?**

There are five major problems with the concept behind programs like "Total Information Awareness" and CAPS II:

- **It would kill privacy in America.** Under this program, every aspect of our lives would be catalogued and made available to government officials. Americans have the right to expect that their lives will not become an open book when they have not done, and are not even suspected of doing, anything wrong.
- **It harbors a tremendous potential for abuse.** The motto of the TIA program is that "knowledge is power," and in fact the keepers of the TIA database would gain a

tremendous amount of power over American citizens. Inevitably, some of them will abuse that power. An example of the kind of abuses that can happen were chronicled in a July 2001 investigation by the Detroit Free Press (and December 2001 followup): the newspaper found that police officers with access to a database for Michigan law enforcement had used it to help their friends or themselves stalk women, threaten motorists, track estranged spouses ( even to intimidate political opponents. Experience has shown that when large numbers of Americans challenge the government's policy (for example in Vietnam), some parts of the government react by conducting surveillance and using it against critics. The unavoidable truth is that a super-database like TIA will lead to super-abuses.

- **It is based on virtual dragnets instead of individualized suspicion.** TIA would represent a radical departure from the centuries-old Anglo-American tradition that the police conduct surveillance only where there is evidence of involvement in wrongdoing. It would seek to protect us by monitoring everyone for signs of wrongdoing - by instituting a giant dragnet capable of sifting through the personal lives of Americans. It would ruin the very American values that our government is supposed to be protecting.
- **It would not be effective.** The program is based on highly speculative assumptions about how databases can be tapped to stop terrorism, and there are good reasons to suspect that it would not work at all (see below).
- **It fails basic balancing tests.** The benefits of this program in stopping terrorism are highly speculative, but the damage that it would do to American freedom is certain.

### **Why would TIA be ineffective?**

There is no question that if government agents track the lives and activities of everyone, they will probably experience some marginal improvement in their ability to stop terrorism - though even a perfect totalitarian society could not stop every attack (the Nazis were unable to stop attacks by the Resistance in France and other occupied nations during World War II, for example). And there is no question that many other, more direct steps that the U.S. is taking will significantly improve our security. The real question is how much additional safety would a TIA program bring us over and above all the other steps we're taking (tightened borders, improved overseas intelligence, increased airport security, etc).

There is good reason to think the answer is: not much at all. TIA is based on the dubious premise that "terrorist patterns" can be ferreted out from the enormous mass of American lives using techniques known as "data mining" that try to identify hidden patterns in large masses of data. What attracts proponents of this scheme is that data mining has proven very successful in some commercial contexts, such as the discovery of suspicious spending patterns that indicate credit card fraud. The problem is that in order to be effective, data miners need an enormous amount of sample data to work from. Credit card companies experience a vast amount of fraud, which allows them to go back and find patterns of behavior that are associated with it. But as horrific as the 9/11 attacks were, there have been very few overall incidents of terrorism within the United States in the recent past, so it is difficult to understand how these programs will be able to identify true patterns of suspicious

behavior, and easy to imagine how they will simply end up reflecting the beliefs and prejudices of their programmers about what that behavior looks like (and there's no need to sift through data about millions of citizens to do that).

In fact, a program like TIA could actually reduce our security by draining resources from more effective measures like improved collection of on-the-ground foreign intelligence.

In the wake of the September 11 attacks, numerous intelligence experts declared that the government's problem was a failure to sift targeted intelligence information from the masses of useless data. The TIA solution to that problem would be to exponentially increase the amount of junk data that the government collects. You don't find a needle in a haystack by bringing in more hay.

If TIA is implemented, it will probably fail at preventing the next terrorist attack. But once created, that kind of failure is unlikely to lead to the program being shut down. Instead, it will probably just spur the government into an ever-more furious effort to collect ever-greater amounts of personal information on ever-more people in a vain effort to make the concept work. We would then have the worst of both worlds: poor security and a super-charged surveillance tool that would destroy Americans' privacy and threaten our freedom.

### **What can I do to help stop this program?**

There are at least four things you can do to help stop the blatantly un-American goal of "Total Information Awareness"

- Educate yourself about this program and tell your friends about it.
- Use the ACLU's "Action Alert" page to send a free and easy fax to President Bush asking him to pull the plug on this research.
- Let your member of Congress know how you feel (locate your member here and check out tips on writing your elected representatives.
- Support the ACLU's efforts to fight this program by joining us.

For more on TIA see the ACLU analysis: Is the Threat From TIA "Overblown"?

Copyright © 2003 American Civil Liberties Union  
Reprinted for Fair Use Only.

<http://www.ratical.org/ratville/CAH/TIAprogram.html>