Is the Threat From "Total Information Awareness" Overblown?

By Jay Stanley

18 December 2002

ACLU

Since the Pentagon's "Total Information Awareness" entered the news recently, the Pentagon, the conservative think tank The Heritage Foundation and others have begun claiming that the furor over the program is based on an exaggerated fears about what it would do. However, a look at Pentagon statements and documents about TIA issued before the furor erupted shows that public concern is entirely justified.

The overall concept is clear. "The purpose of TIA would be to determine the feasibility of searching vast quantities of data to determine links and patterns indicative of terrorist activities," as Under Secretary of Defense Edward C. "Pete" Aldridge put it. [1] And a close examination of existing public material on TIA makes several other points clear: the goal is to collect information about everyone, not just specific targets; privacy protections promised by Pentagon officials cannot be relied upon; and existing legal protections for privacy cannot be relied upon.

The TIA program would affect everyone

First, it is clear that TIA intends to leave no stone unturned when it comes to gathering personal information. . The director of theprogram, Adm. John Poindexter, explained what TIA is all about at a DARPA conference in Anaheim, California in August 2002. [2] He told his audience:

> We must be able to *detect*, classify, *identify*, and *track* terrorists. . . .
>
> Certain agencies and apologists talk about connecting the dots, but *one of the problems is to know which dots to connect*. The *relevant information* extracted from this data must be made available in large-scale repositories with enhanced semantic content for easy analysis to accomplish this task. . . .
>
> [Terrorists'] low-intensity/low-density form of warfare has an information signature. We must be able to pick this signal out of the *noise*.

Clearly, if you don't know who the terrorists are, then to "identify" or "detect" them (to know which "dots to connect" (you must sort through the lives and activities of everyone. And when Poindexter talks about "noise," what he is referring to is personal information

about the lives of millions of innocent people. The only way to separate "relevant information" from that "noise" is to look at all of it.

In addition, "tracking" terrorists would most likely involve recording and retaining the activities of everyone, because the authorities are going to want the ability to look at what a suspected terrorist was doing before they recognized him as a suspect. In fact, that may be TIA's primary role, since once a person is identified as a suspected terrorist, they can be followed, bugged, spied upon, videotaped, and (given proper evidence) arrested; the authorities are unlikely to rely on the TIA to keep tabs on someone they think is a terrorist.

Tracking all the pieces all the time

Not only is it is clear that the program's goal is to collect specific data on many people, but it is also seen as collecting a LOT of information on those people. As Poindexter said,

> One of the *significant new data sources* that needs to be mined to discover and track terrorists is the *transaction space*. If terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions and they will leave signatures in this information space.

"Transaction space" appears to be a fancy way of saying "all the records of everything that everyone is doing." The list of "transaction categories" that DARPA envisions using in the TIA system is "Financial, Education, Travel, Medical, Veterinary, Country Entry, Place/Event Entry, Transportation, Housing, Critical Resources, Government, Communications." [3] Given that computers are increasingly being used to track and record our activities in all these areas, TIA's potential as an all-encompassing government surveillance tool should be taken with the utmost seriousness.

According to the TIA Web site, the program is aiming at a "full-coverage database containing *all information relevant* to identifying" potential terrorists and their supporters. [4] What information is "relevant" to this task in DARPA's view? A talk given by TIA manager Ted Senator at the August 2002 conference in Anaheim provides the answer. [5] Illustrating the potential of monitoring people's activities, he pointed out that to arrange his attendance at the DARPA conference, he had made more than 25 "transactions."

> I had to arrange for airline tickets and hotel reservations and airport transportation. I sent e-mails to colleagues and to friends to coordinate schedules. I had to coordinate schedules with my wife and children. I checked airline reservation web sites for flight options. I registered. And I must have sent and received innumerable e-mails with various drafts of this talk.

"That is what EELD is all about," Senator said. "Developing techniques that allow us to find relevant information (about links between people, organizations, places, and things (from the masses of available data, putting it together by connecting these bits of information into patterns that [can] be evaluated and analyzed." Senator also explained that:

> Traditional fraud detection techniques look for outliers, i.e., behavior by individuals that is unusual according to some statistical measure. . . . What we need to look for to detect behavioral patterns representative of asymmetric threats [i.e. terrorism] is not outliers, but what I like to call "in-liers." . . . The most dangerous adversaries will be the ones who most successfully disguise their individual transactions to appear normal, reasonable, and legitimate.

In other words, we have the answer to the question of what information the TIA program believes is "relevant" to the discovery of hidden terrorist behavior. It is records of individual transactions that are "normal, reasonable, and legitimate."

Senator also argues that the program's task is "much harder than simply finding needles in a haystack." Rather, "our task is akin to finding dangerous groups of needles hidden in stacks of needle pieces." His conclusion? "In principle at least, we must track all the needle pieces all of the time and consider all possible combinations."

Don't count on privacy protections

In his Anaheim speech, Admiral Poindexter mentions the importance of privacy:

> The Information Awareness Office at DARPA is about creating technologies that would permit us have both security and privacy. More than just making sure that different databases can talk to one another, we need better ways to extract information from those unified databases, and to ensure that the private information on innocent citizens is protected. The main point is that we need a much more systematic approach.

No one who follows privacy, however, is impressed by bland, nonspecific reassurances about how privacy will be protected. For example, many corporate privacy policy statements that tell customers in legalistic language that their information will not be kept at all private start off with the statement "We respect your privacy."

In addition, to talk about preserving privacy in the context of a project that seeks to find "a much more systematic approach" to linking together all available sources of data on individuals' lives, would be like Dwight D. Eisenhower saying "we need to make sure no one gets hurt" while planning the D-Day invasion. The stated goal stands in massive contradiction to the overall project. Poindexter told his Anaheim audience that:

> While our goal is total information awareness, there will always be uncertainty and ambiguity in trying to understand what is being planned. That's why our tools have to build models of competing hypotheses. That is, we need to bring people with diverse points of view together in a collaborative environment *where there is access to all source data*, discovery tools and model building tools. . . . And tools have to make the analysis process more efficient, *to properly explore the multiple possibilities.*

That is not the language of a privacy-protecting vision. To "explore the multiple possibilities," analysts will need to be able to run down hunches (whatever mix ofpolitical bias, prejudice, and real evidence those hunches may involve (by surfing through Americans' private lives. It is the computer-data equivalent of letting police roam around our neighborhoods looking into our houses using see-through X-ray scanners in a search for terrorists. It crosses the line into an egregious violation of American values.

The contradiction between this program and the goal of privacy is made clear by its very name. It is not "Anti-Terrorism Information Awareness," or "Suspicious Information Awareness," but "*Total* Information Awareness."

Good intentions may abound at DARPA, but the fact is that the entire point of TIA is to

monitor people's personal lives, and once such a tool becomes operational, every institutional incentive will press in the direction of reducing privacy protections and increasing intrusiveness. Once brought into existence, this tool for total surveillance will create its own bureaucratic and political imperatives. Just as we don't trust police and prosecutors to protect the rights of people accused of crimes (we have evolved an elaborate system of judges, juries, and procedures to do that based on centuries of experience (so too would the goals and incentives of a TIA program destroy privacy unless there are carefully constructed institutional checks and balances to protect it.

Unfortunately, no such measures are in sight. The ACLU is having to fight an extensive legal battle with an uncooperative Justice Department just to gain basic information about how *existing* surveillance laws are being interpreted and used. Americans should pin few hopes on an active TIA being subject to proper public oversight.

Open season on information about our lives

"How is this not domestic spying?" a reporter asked Pentagon officials at the November 20 press briefing. "You have these vast databases that you're looking for patterns in. Ordinary Americans. . . their transactions are going to be perused." Under Secretary Aldridge replied that the military was just developing a tool:

> It is technology. Once that technology is transported over to the law enforcement agency, they will use the same process they do today. . . . They would have to go through whatever legal proceedings they would go through today to protect the individuals' rights.

The problem with that argument is precisely that there are no "legal proceedings" or laws covering law enforcement access to much of the kind of data that TIA would utilize (and such laws would almost certainly be opposed by the law enforcement and intelligence bureaucracies. Most of the interactions and "transactions" in Americans' lives are not with the government, but with corporations and other private entities, who therefore hold most of the details about individuals' lives. Among the data sources listed by the TIA, many (financial, medical, travel, place/event entry, transportation, housing, and communications (are kept by the private sector. That list covers much of what is important and private about people's lives. And some companies, known as "data aggregators," are in the business of compiling huge databases about individuals' buying habits and other information.

Unfortunately, the rules that protect the privacy of such information from government are very weak. Already, the FBI is known to have a contract with data aggregator Choicepoint that allows agents to look at a vast amount of personal information about individuals. The legality of such access is far from clear under the Privacy Act of 1974, but they are proceeding full speed ahead, and refusing to provide information about their practices. There's no need for the government to compile dossiers on individuals if the private sector can do it for them.

One of the reasons that the law is so undeveloped in this area is that it was never an issue; until recently our privacy has been protected by the fact that it was difficult or impossible to bring together information about individuals collected by different parties at different times and in different places. But advancing computer technology is increasingly allowing for that

to happen. Officials can increasingly access a frighteningly complete and intrusive view of an individual's life without the carefully developed legal protections that have long restrained direct government spying. It is TIA's intention to exploit this brand-new potential that is cause for so much concern.

Admiral Poindexter confirmed the accuracy of this view of TIA's aims. One of its goals, he said in Anaheim, is to "develop ways of treating the world-wide, distributed, legacy databases as if they were one centralized database." That means creating computers that can talk to all the existing databases in the world with such ease and fluidity that for all practical purposes, they form a single database. Even if that database is "distributed," or scattered around different computers, it will have all the power (and potential for abuse (of one giant database. And that would mean a true end to privacy.

For more information on the civil liberties problems with TIA, see the ACLU's Q&A on Total Information Awareness.

NOTES

1. Under Secretary of Defense for Acquisition, Logistics, and Technology Edward C. "Pete" Aldridge, statement read to reporters at a Pentagon press briefing, Nov. 20, 2002. Transcript available online at http://www.fas.org/sgp/news/2002/11/dod112002.html.

2. Emphasis added in all quotes. A copy of Poindexter's prepared remarks is online at http://www.fas.org/irp/agency/dod/poindexter.html.

3. TIA program graphic, online at http://www.darpa.mil/iao/TIASystems.htm.

4. http://www.darpa.mil/iao/Genisys.htm.

5. Senator is head of the "Evidence Extraction and Link Discovery Program" (EELD), a part of TIA. His comments are posted online at http://www.darpa.mil/DARPATech2002/presentation.html.