The Culture of Surveillance: G-Men Redux and Total Information Awareness

ABSTRACT
Part of the U.S. Defense Advanced Research Projects Agency’s Information Awareness Office, the Total Information Awareness (TIA) project, enacted in the wake of September 11th, aims to capture the “information signature” of citizens suspected of terrorism or criminal acts. Technical means (including computer algorithms and human analysis) afford the government the ability to track those involved in “low-intensity/low-density” forms of warfare and crime, its ultimate goal to track individuals through collecting as much information about them as possible. Various public interest groups have criticized this initiative, particularly on the basis of privacy and security risks, identity theft, misuse of information, and overt citizen surveillance. This article will provide an overview of TIA and situate it within an ongoing political economy of the military-industrial complex, now revamped for an emerging security industry.

Introduction
Post September 11 has unleashed a cavalcade of new legislation in the United States and Canada whose goals are to protect and promote security measures in light of purported terrorist threats. In the U.S., the PATRIOT Act (full name: “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”) was introduced in October 2001, and signed into law on October 26 (U.S. Congress 2001). Its quick approval, without House and Senate reports or widespread public hearing, has been criticized by public interest groups for its expansion of governmental investigative powers, especially on the Internet. Various PATRIOT Act provisions address complex and fundamental constitutional issues, including the protection of individual liberties.
As part of Canada's new plan to combat terrorism, Bill C-36 (the "Anti-Terrorism Act") has also, like its U.S. counterpart, become the object of debate. Controversial aspects of this omnibus Bill include a widening of the definition of what constitutes a "terrorist," 72-hour preventative arrests of individuals suspected of being involved in a terrorist activity, and changes to the Privacy Act and the Access to Information Act that would prohibit the disclosure of information to Canadians. Bill C-36's quick tour of the House of Commons and Royal Assent on December 18, 2001 was predicated upon Canadians' willingness to compromise their civil rights in exchange for greater security.  

This article will examine one of the more draconian proposals, the Total Information Awareness Project (TIA), an initiative of the U.S. Defense Advanced Research Projects Agency (DARPA). Highly sophisticated and elaborate technical means will allow the government to track people involved in "low-intensity/low-density" forms of warfare and crime, with the end result the collection of an intense dossier of information on suspected individuals. First, the TIA project will be described, and then the views of several public interest groups who have criticized this initiative on the basis of privacy and security risks, identity theft, misuse of information, and overt citizen surveillance, will be discussed. This article will then situate TIA within a regime of command-control communication computer systems with origins dating back to the Cold War and Reagan's Star War (Strategic Defense Initiative) project in the 1980s, and to what Der Derian (2002) now refers to as the new "military-industrial-media-entertainment network." It will conclude with a brief political economy of the current military-industrial complex, which integrates the security industry and other major players in the computer industry.

**Total Information Awareness**

Our nation is in a new kind of war. We need an innovative tool such as TIA for our defense. This war is being fought on our soil, and we are fighting for our existence. There is no truce or quarter being offered in this conflict. We cannot afford to decide that it is costing too much or making us too uncomfortable, and shy away from the task at hand. We must win this war. Long after we have defeated the current enemy, we will need to stay vigilant and armed to ensure new enemies do not strike.

– Jeff Carley 2002; he is a chief technology officer for Engedi Technologies Inc., a Virginia-based company developing security products for network infrastructure.

The Total Information Awareness Project is the brainchild of John Poindexter, the former national security advisor under Ronald Reagan. During his tenure in the Reagan Administration, Poindexter was involved in the Grenada invasion and the bombing of Libya (Safire 1987) as well as "the modernization of the White House Crisis Management Center—also known as the Presidential Emergency Operations Center—in the Executive Office Building. It was equipped with video equipment, computers and electronic message systems—a more novel concept then—to connect to the Pentagon and State Department and intelligence agencies" (Markoff 2003). Poindexter is more infamously known as a key player in the Iran-Contra investigation (in which sales of
arms to Iran were used to finance rebels fighting in Nicaragua at a time when Congress had barred such assistance), and he was convicted in 1990 on five counts of lying to Congress, making false statements, destroying documents and obstructing inquiries. It is alleged that he created a back door called a “private blank check,” to circumvent normal White House e-mail channels and to facilitate his oversight of Col. Oliver North’s illegal activities (Ibid). Always the technocrat, Poindexter was, throughout the 1990s, a military consultant through Symantec Inc., where he promoted his vision of the Command Post of the Future project, an initiative to provide information to military planners via computer networks.

The TIA project is situated in the U.S. Defense Advanced Research Projects Agency’s (DARPA) Information Awareness Office, and its goals are 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.” TIA will “imagine, develop, apply, integrate, demonstrate, and transition information technologies, components, and prototype closed-loop information systems that will counter asymmetric threats by achieving total information awareness that is useful for preemption, national security warning, and national security decision making.” (<http://www.darpa.mil/iao/>)

Dissecting this nomenclature, it appears that asymmetric threats here refers to terrorism, “a threat characterized by collections of people loosely organized in shadowy networks that are difficult to identify and define” (ibid). DARPA contends that their creation of a counter-terrorism information system will enable the detection, classification, and identification of foreign terrorists, so that the U.S. intelligence community can preempt and defeat terrorist attacks in a timely fashion. The prototype system to be developed focuses on language translation technologies, data search and pattern recognition technologies, and advanced collaborative and decision support tools.

TIA consists of an integration of technologies already developed and in use by DARPA, focusing in particular on the compilation of databases and data mining techniques that can sort through a wide variety of information and transaction data (medical records, financial records, education records) as well as allowing for the integration of intelligence material. Patterns and associations from this panoply of information can then be assessed, allowing intelligence officers to detect potential terrorists and terrorist activities.

Several discrete projects within TIA include:

**Babylon**—the development of a two-way natural-language speech translation interface, to be used for force protection, refugee processing, and medical triage. Focus will be on four languages: Pashto, Dari, Arabic, and Mandarin.

**Bio-ALIRT** (Bio-event Advanced Leading Indicator Recognition Technology)—the development of information technologies capable of detecting the covert release of biological pathogens. This will be accomplished through monitoring “non-traditional data sources such as animal sentinels, behavioral indicators, and pre-diagnostic medical data.”
Communicator—the development of "dialogue interaction" technology for "warfighters" to obtain information in the "battle space."

Effective Affordable Reusable Speech-To-Text (EARS)—development of speech-to-text (automatic transcription) technology.

Evidence Extraction and Link Discovery (EELD)—"development of technologies and tools for automated discovery, extraction and linking of sparse evidence contained in large amounts of classified and unclassified data sources" in order to put together patterns of terrorist relationships and activities.

Genisys— compilation of a "full-coverage database containing all information relevant to identifying: potential foreign terrorists and their possible supporters; their activities; prospective targets; and, their operational plans."

Human ID at a Distance—development of automated biometric identification technologies "to detect, recognize and identify humans at great distances."

Civil Liberties and TIA

When initially announced to the public, the website of the Information Awareness Office emblem featured a human eye, embedded in the peak of a pyramid, scanning the globe, with the motto "scientia est potentia," or "knowledge is power." Criticized by many (a Washington Post editorial questioned Poindexter's logo for "his tact and taste" (2002), the logo has since been replaced by a more sedate graphic.

The public reception over TIA has been anything but welcoming. Editorials in the major newspapers—The Washington Post and The New York Times, as well as regional newspapers—have criticized Poindexter's folly. It has been dubbed "Orwellian" and a project leading to a surveillance state. The privacy implications of TIA trolling through commercial and private databases to compile information dossiers on ordinary citizens have left many unnerved. One person started up the John Poindexter Awareness Page (<http://www.breakyourchains.org/john_poindexter.htm>) where ordinary citizens are encouraged to write in reports of Poindexter sightings. A diverse nonpartisan coalition of organizations wrote to Senators Daschle and Lott, asking them to curtail TIA because of its massive privacy implications and lack of public accountability. What was remarkable about the letter was that it was signed, not just by computer civil libertarian groups (including the Electronic Privacy Information Centre, Electronic Frontier Foundation, and the Privacy Rights Clearinghouse), but by consumer groups and academics; and, oddly, Phyllis Schlafly of the conservative Eagle Forum, and representatives from People for the American Way and the Libertarian Party.2

The estimated $240-million project (for fiscal years 2001-2003) has not been without critics in the government. In January 2003 the Senate unanimously passed an amendment to the TIA omnibus spending bill that would bar deployment and limit research of the project. Two Advisory Councils (an internal oversight board and an outside advisory committee) were also established by the Defense Department to make sure that
TIA follows U.S. constitutional law, U.S. statutory law, and American values related to privacy (Clymer 2003).

TIA will rely on computer-based pattern recognition techniques known as data mining. This is a set of statistical techniques used by scientists as well as by marketers searching for potential customers. Multiple databases will be combed to piece together evidence of terrorist activity; for instance, air travel and car rental records, work permits, flight school registrations, etc. However, this technology has been particularly criticized for its security, privacy, and economic risks. Data mining from multiple databases, often containing sensitive and personal information, can lead to security breaches, including identity theft and malicious hacks. Fair Information Practices, outlined in the 1974 Privacy Act, would be compromised, as oversight, control, and protection from misuse would be heightened. Data mining technology also gives off too many false positives, so the accuracy of the information collected is often not too intelligent.

Rosen (2002) shows that the companies Accenture and HNC Software are testing an airport profiling system through data-mining and predictive software. Various attributes (living arrangements, real estate information, travel history, financial, demographic, and other personal information) would be collated to create a “threat index based on his or her resemblance to a terrorist profile. Passengers with high threat indexes will be flagged as medium or high risks and will be taken aside for special searches and questioning.”

Civil libertarians and computer scientists argue that use of such data mining techniques would not thwart terrorists (as they would learn how to bypass the system to avoid detection), but rather threaten to create a more heightened surveillance state. Lyon argues that all societies dependent on ICTs for administration and control are surveillance societies: “routine mundane surveillance, usually mounted by agencies and organizations that are geographically remote from us is embedded in every aspect of our life,” (2002: 1) but that the increasing globalization of our risk societies, the everyday monitoring, and the ease and speed with which it can be shared across multiple borders and interoperable systems can produce ethical quandaries.

Gandy (1993), in his study on the political economy of personal privacy, refers to the panoptic sort, which is characterized by the collection and use of personal information: “[it is] a complex discriminatory technology. It is panoptic in that it considers all information about individual status and behavior to be potentially useful in the production of intelligence about a person’s economic value. It is a discriminatory technology because it is used to sort people into categories based upon these estimates” (1996: 133). ICTs are essential not only for creating the panoptic sort, but also for “the analytic approaches that differentiate, classify, segment, and target individuals and groups upon the basis of models, assumptions, and strategic orientations that demand the maximization of profit and the minimization of risk” (Ibid: 134).

Although Gandy’s panoptic sort is controlled by consumer information collected and controlled by the capitalist marketplace, we could consider TIA to be a hyper-panoptic sort, as it relies on both the collection of private and public information, and the analysis, classification, and assumed qualities of citizen behavior—in this case not as
consumers, but as potential terrorists. And, such classification, as Foucault (1979) argues, involves power.

Poindexter has argued that because TIA would look only “for certain patterns in commercial database—not create any centralized record-keeping system of American citizens’ activities—it would not violate civil liberties” (Markoff 2002). And TIA officials downplay the use of data mining fears, saying that they are instead developing a series of templates, or “likely attack” scenarios, which would help TIA decide which databases to investigate (Harris 2003).

Towards a Political Economy of the Military-Industrial-Security Complex

In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military industrial complex. The potential for the disastrous rise of misplaced power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together.

– Dwight D. Eisenhower, Public Papers of the Presidents, Dwight D. Eisenhower; 1960: 1035-1040

Eisenhower’s words seem prescient today, and a stark contrast to the Bush Jr. Administration and their visions of nationhood via Homeland Security. Throughout the years, the military has exerted an influence on the key developments in information and communication technologies (ICTs) through design, development, and dissemination, with many of the technologies eventually entering the civilian economy.

As Mosco (1989) has documented, the Pentagon and the electronics and computer industries have always had a tight relationship, evidenced by the creation of DARPA and the military consumption of computer products (semiconductor chips) used to develop the Intercontinental Ballistics Missile (ICBM), and other weapons systems. Historian FitzGerald (2000) has documented Reagan’s multi-billion dollar missile defense system (the Strategic Defense Initiative, or as it was popularly known—Star Wars), and his rhetorical strategies of morality and patriotism to convince the American public to combat the “Evil Empire” of the Soviet Union. As Mosco argues, this initiative provided “the primary legitimate means of providing direct government funding for corporate research and development in the United States,” alongside “business pressur-[ing] government to maintain a permanent war economy because a war economy channels a stable flow of guaranteed profit” (1989: 158-159).

Knowledge institutions, including elite universities, both public and private, have always reaped profits through DOD contracts. Schiller (1973), writing in the early 1970s when the Vietnam War was a contested national debate, argued that the knowledge industry consisted of a military-corporate component, wherein military contracts to public and private universities influenced the types of research conducted on campuses. We
see a revival of this now with the militarization of computer science and engineering. The Center for Public Integrity found that “at least 24 universities received almost $10 million during the last five years to do research on TIA-related projects. Some of the largest grants went to Cornell University, Columbia University and University of California, Berkeley and dealt with the TIA’s language translation program” (Mayle and Knott, 2003).

From anti-communism sentiments to our contemporary anti-terrorism hyperbole punctuated by “Operation Enduring Freedom,” the stimulation of public anxiety has enabled a veritable industry to build up around creating security technologies. Small start-ups and venture capital seed funding that used to go towards developing security functions for e-commerce applications have now, because of the dot.com bust and federal imperative to create “homeland security,” been directed towards security technologies for the military-industrial complex. A Freedonia Industry study on the electronics security industry estimates that in the U.S. alone, sales of these products are forecast to grow 10% per year to 2006, up to $11.5 billion. Products include access controls and biometrics, bomb and metal detection equipment, and electronic article surveillance system.

TIA does rely on earlier commercial systems; for instance, Chalemien cites the example of a software collaboration program called Groove, developed in 2000 by Ray Ozzie, a well-known software designer who is the inventor of Lotus Notes. “Groove makes it possible for analysts at many different government agencies to share intelligence data instantly, and it links specialized programs that are designed to look for patterns of suspicious behavior.” (2002) As well, TIA utilizes Extended Markup Language (XML), an Internet flexible text format designed for wide-scale electronic publishing. Created by a bevy of software designers in Silicon Valley and at the dominant companies, including Microsoft, Sun Microsystems and I.B.M., it has become an indispensable aspect of Internet publishing and e-commerce (see the World Wide Web Consortium XML page at <http://www.w3.org/XML/>).

Outsourcing Big Brother has also become Big Business. DARPA’s BAA 02-08 Information Awareness Proposer Information Pamphlet asks private companies to provide “innovative research proposals in the area of information technologies that will aid in the detection, classification, identification, and tracking of potential foreign terrorists and to develop options to prevent their terrorist acts” (see <http://www.darpa.mil/iao/BAA02-08.pdf>). Defense contractors, including Lockheed Martin, Boeing, Northrop Grumman, Raytheon, General Dynamics, and TRW have reaped billions in Pentagon awards (see the Federation of American Scientists at http://www.fas.org/asmp/profiles/top10fy02.html).

The Center for Public Integrity has documented some of these DARPA contracts awarded to the major players (Mayle and Knott, 2003). These include:
Booz Allen & Hamilton
(<http://www.boozallen.com>)
This strategic management and consulting firm was awarded a $1,500,000 increment as part of a $62,876,051 cost-plus-fixed-fee contract for total information awareness support on Nov. 7, 2002. (Defense Link, DOD News, <http://www.defenselink.mil/news/Nov2002/c11122002_ct577-02.html>)

Lockheed Martin Corporation
(<http://www.lmasc.com>)
A long-time player in producing and manufacturing aerospace products, they received 23 contracts for TIA for a total of $27 million.

The Schafer Corporation
(<http://www.schafercorp.com>)
A scientific analysis and engineering company, whose programs include airborne laser, joint theater air and missile defense, and national missile defense, they were awarded 9 contracts for a total of $15 million.

SRS Technologies
(<http://www.srs.com>)
Involved in systems engineering, their contracts total a little under $5 million.

Syntek Technologies
(<http://www.syntek.org/Overview.htm>)
The former employee of Poindexter, which helped develop Project Genoa, a project of TIA, they have been awarded $2 million.

Hicks & Associates Inc.
(<http://www.hicksandassociates.com>)
A national security consulting service, they are receiving a “3,600,000 increment of a $19,300,000 other transaction for prototypes agreement for feasibility and development of a closed-loop, end-to-end prototype system for early warning and decision-making including the integration of previously developed technologies” (Defense Link, <http://www.defenselink.mil/news/Dec2002/c12162002_ct637-02.html>).

Less overt relationships exist amongst members of the Republican Party and Bush administration through the Carlyle Group, an equity investment firm with billions of dollars in military and aerospace assets (<http://www.thecarlylegroup.com>). Carlyle's Chairman is former IBM CEO Lou Gerstner, Chairman Emeritus is Frank Carlucci, Secretary of Defense in the Reagan administration, and Senior Counselor is former Secretary of State James Baker. George Bush Sr. is also affiliated with the group, and rumors have swirled about their relationship with Bin Laden (Burkeman and Borger, 2001).

Silicon Valley firms are also involved in turning their commercial applications into new markets for the federal government. Oracle Corporation now has a program on homeland security and disaster-recovery solutions. One such program, a “bioterrorism shield,” is being marketed to hospitals allowing them to “report incidents of suspicious diseases like anthrax, smallpox and Ebola to a central database. The program can then send out
e-mail or voice-mail alerts to law-enforcement officials if it detects suspicious patterns of diseases anywhere in the country” (Rosen, 2002).

What happens when these technologies, purportedly to be used for national security, became a mundane and integral part of our daily lives? Gandy writes presciently that the use of these systems as a routine aspect of government agencies will increase the likelihood that they will “soon become available as off-the-shelf commodities for use in the commercial sector” (2002, 11). Indeed, online marketing practices targeting e-commerce consumers are an integral component of the capitalist surveillance imperative (Campbell and Carlson, 2002). In either context, no social impact assessments accompany the design, development, and deployment of these technologies. The architectural code is divorced from social justice concerns surrounding privacy. And in a troubling twist, in many instances, citizens or consumers are implicated themselves in becoming the objects of such surveillance; whether through participating in online surveys and information gathering, or subjecting themselves to biometric scans for security reasons.

Surveillance, then, can be normalized. And it is not just the “private spaces” of the Internet that we surf that can be targeted. It is also the public spaces in which we reside. CCTV cameras, video feeds linked up to databases, private and public cameras secured on traffic lights, office buildings, residential complexes, in parks and on playgrounds provide many potential opportunities for abuse. As SmithSimon writes, “the technology could easily be used for sexual voyeurism, racial profiling, or to harass gays, lesbians, and transgendered people” (2003, 45).

The Total Information Awareness Program, if left to the devices of the DOD and the Bush Administration, thus poses grave threats to the public interest: to our right to privacy and to our right to assembly; to our right not to be surveilled, and to our right to participate in a democratic society. As Canadians, we might think that we are immune from such a surveillance project, but we must question whether TIA will draw Canada more directly into the U.S. military system. And we must also be very alert to Canada’s response to the war on terrorism. In his annual report to Parliament, Privacy Commissioner George Radwanski warned that “this Government has lost its moral compass with regard to the fundamental human right of privacy” (Privacy Commissioner, 2003). Citing several pieces of proposed anti-terrorism legislation, including the Canada Customs and Revenue Agency’s passenger database, Citizenship and Immigration’s national ID card with biometric identifiers, and the RCMP’s use of video surveillance of public streets, Radwanski ominously predicted that “privacy as we know it will soon become a distant, irretrievable memory.” Privacy is a fundamental human right, and we must be vigilant about maintaining this as an integral part of our public interest.
Notes


References


