The Return of Big Brother?

Privacy, Surveillance Technologies, and Ethics After 9-11"

Reg Whitaker

A Lecture co-sponsored by the Ethics

Centre and the Glasmacher Lectures

of Saint Paul University

14 March 2003

FAUST: By spying, your all-knowing wit is warmed?

MEPHISTOPHELES: Omniscient? No, not I; but well-informed.

The terrorist attacks of Sept. 11, 2001, and the declaration of a War on Terrorism, have raised the spectre of a global surveillance regime. The technological capacity to achieve a global surveillance regime has been known for some time. The last two decades of the twentieth century witnessed remarkable developments in surveillance technologies. The daily lives of people everywhere, but particularly in the most industrially developed nations, are now tracked and recorded. Electronic eyes scan the globe, from closed circuit cameras on the ground, to satellites gathering sophisticated imagery from space. Voice communication is scooped out of the sky by electronic listening posts. Sophisticated

search engines troll through e-mail traffic and internet use. The global positioning system based on satellites can yield the precise location of targeted individuals anywhere on earth. Unique biometric identifiers such as palm and finger prints, iris patterns, facial and gait characteristics, DNA sequencing, are increasingly being recorded and stored in data banks – and demanded to gain access to services or pass security screenings. Virtually every daily economic transaction adds to an electronic trail that can potentially construct a unique social profile of an individual. Detailed medical records and significant genetic information can profile individuals in a remarkably intimate manner.

What is particularly alarming to privacy advocates is that the new information technologies, based on the universal language of digitization, permit the seamless transfer and matching of information gathered by different agents for different purposes. Data bases can 'talk' to each other, and, in so doing, create the capacity for decentralized 'dataveillance', a surveillance society in which the 'files' exist in no central location, and are perhaps under no central control, but which in their totality may exercise far more intrusive capacity to gaze into the private space of individuals than the Big Brother surveillance state of the past. Yet these same technologies offer numerous benefits that must be balanced against the threats they pose to privacy: to take one instance alone, the potential benefits to health of detailed medical and genetic data bases are immense. The same developments that alarm some, excite others. Indeed, most typically, they both alarm and excite the same people.

The political and administrative problem of privacy protection in the era of dataveillance has generally been posed as: how best to constrain and control this technical potential so as protect a reasonable degree of personal privacy, while at the same time retaining the economic and social benefits promised by the new technologies?

Prior to 9/11, there seemed good reason to believe that there were structural impediments to total surveillance. The new information technologies, although often originating in the defence sector, owe their rapid global diffusion primarily to private sector research, development, and marketing. Their commercial potential had been best exploited by the corporate sector, with governments by and large reaping the benefits as technological spinoffs. But a paradox had appeared in the 1990s. The toolbox of surveillance was increasing exponentially while the totalitarian surveillance state which had been so threatening a feature of the twentieth century, whether in fascist or communist form, was in dissolution, and even the liberal capitalist state that had borrowed, in less virulent form, many of the surveillance capacities of the authoritarian state, appeared to be in retreat before the forces of the market.

If states collect and use information on their citizens primarily as a means of social and economic

control, corporations collect personal data primarily for marketing purposes. There is a long tradition, especially in the US, of resisting government threats to personal privacy. More recently, different concerns have been raised about threats to privacy arising from the vast, unregulated, and rapidly accumulating corporate databanks. These concerns can be best described as a shift from the Big Brother surveillance state to the Little Brothers surveillance society.[1] Legal responses have varied. Europe and Canada have adopted public regulatory regimes that stipulate that personal data collected by private entities for a specific commercial purpose may not be sold or traded to third parties without the express consent of the individuals from whom the information was drawn. The US, with its anti-government traditions, has so far tended to rely more on corporate self-regulation, enforced largely by private litigation. In both cases, the emphasis is on firewalls separating public from private data collections, and separating different private data collections from each other. In the absence of effective barriers, data matching and linkage quickly threatens personal privacy. Yet despite the ominous growth trajectory of panoptic technologies, the de-centered and dispersed quality of the information gathered by the electronic eyes and ears diminished their totalizing potential. Nobody, public or private, seemed to have the will or capacity to put it all together – until 9/11.

Even with the attention paid to the private sector, it was already apparent well before 9/11 that states, and the United States pre-eminently among them, did have some impressive, but underused, surveillance capacity. Two examples illustrate the potential for a renascent Big Brother state. Since the late 1940s, the English-speaking countries under the leadership of the US National Security Agency (NSA), have maintained an extensive electronic eavesdropping partnership known as the UKUSA alliance. During the Cold War, listening posts across the globe closely monitored communications within the Soviet Bloc. Today the UKUSA countries tap into the Intelsat communications satellite system that relays most of the world's phone calls, faxes, telexes, internet and e-mail communications around the world. A system called ECHELON links all the computers among the UKUSA agencies using a set of keywords in a Dictionary contributed by all the agencies; flagged messages are automatically routed to the country or countries that entered the particular keyword flag. In the US, the FBI had, before 9/11, begun deploying CARNIVORE, a super search engine which, when installed on internet service providers, is capable of trolling through e-mail traffic and flagging communications of interest to the agency based on the identities of senders and receivers, keyword recognition, etc..

A second example of state surveillance capacity is the machinery for tracking money laundering trails centered in the US Treasury Department in the Financial Crimes Enforcement Network. FinCEN "links the law enforcement, financial and regulatory communities together for the common purpose of

preventing, detecting and prosecuting money laundering and other financial crimes."[2] FinCEN relies on world wide monitoring of large financial transactions, and reportedly has at its disposal sophisticated artificial intelligence software capable of detecting anomalous or suspicious patterns in the vast daily volume of transactions, flagging transactions that might require closer attention, or criminal investigation. Technology permits the instantaneous flow of capital across national borders by computer key stroke, which has assisted in the rapid development of transnational financial networks. Governments, the bankers and financiers assert, cannot interfere effectively in this globalizing process, and should stay out. Yet these networks are also threatened by illicit financial flows, funding criminal or terrorist enterprises, and here the private sector needs, and demands, the intervention of governments. The same technologies that foster licit financial flows, also enable national states working together, under US leadership, to monitor and investigate illicit flows.

Prior to 9/11, these powerful state surveillance systems faced certain limitations, both legal and political. Each of the participating UKUSA agencies was constrained by domestic law or practice from listening in on its own citizens. The awesome potential of the ECHELON system drew the critical attention of the European Parliament, especially of its French members who complained about a global 'Anglophone spy network' that might be used against European economic interests.[3] FinCEN's potential was limited by the reluctance of many countries to cooperate fully with new disclosure laws, and of many transnational financial corporations to open their books and their clients' financial data, to Uncle Sam's prying eyes. Nevertheless, the need to control the dark side of globalization, whether organized criminal or terrorist networks, had given greater urgency to the deployment of international policing and surveillance. The return of Big Brother could be discerned, just over the horizon.

HOW 9/11 DIFFERS FROM PAST GLOBAL CRISES

Like the two most recent historical antecedents of this war, World War II and the Cold War, the War on Terrorism has ramifications for domestic politics, especially for civil liberties and minority communities. The forcible relocation of the Japanese populations from the west coast in 1942, and the excesses of McCarthyism in the early Cold War, offer notorious examples of how the search for security can generate injustices. More worrisome is the potential long term damage to the fabric of civil liberties that may persist long after the emergency passes.

The historical cycle in which violent threats generate the expansion of arbitrary and intrusive powers of government is being repeated. Once again, the constitutional protection of rights is being dismissed, sometimes from the highest offices in the USA, as an inconvenient impediment to safety. And yet again a panicked public is encouraged to trust in action over deliberation, results over due process.[4]

In certain ways, the present crisis bears even more dangerous potential than earlier wartime emergencies. The terrorist threat is qualitatively different from the threats posed in previous emergencies. As Washington struggles to find the most effective response to a new, and, in many ways, unprecedented threat, the very novelty and uncertainty of the situation tempts government to reach for new powers, while heedlessly discarding old forms and conventions. Phrases such as ‘thinking outside the box’, and ‘connecting the dots’, may be appropriate for policy makers moving in unfamiliar and uncharted territory, but they can be dangerous guides for encroaching upon rights.

There is much that is novel about the organizational structure and operating methods of the terrorists. Al Qaida is a contemporary product of globalization: flexible, adaptable, diversified, transnational, de-centered, a network of networks. Like transnational organized criminal networks, Al Qaida operates very much as a paradigm ‘new economy’ corporation. As part of the ‘dark side’ of globalization, terrorist networks assiduously cover their global tracks, evading the scrutiny of law enforcement and security agencies rooted in national jurisdictions. As borderless enterprises, they utilize the most up to date technologies of communication that facilitate the instantaneous transfer of ideas, capital, and financial resources across national borders and continents. The intelligence and security failure of 9/11 clearly signaled the need for agencies like the CIA and the FBI to modify, if not reinvent, new and more appropriate intelligence-gathering mechanisms. Just as clearly, emphasis on new information technologies and more intrusive and extensive surveillance was inevitable.

DISAPPEARING BOUNDARIES BETWEEN PUBLIC AND PRIVATE

In response to the borderless terrorist threat, government has tried to dissolve, or at least to weaken, a series of boundaries that had previously been erected to demarcate spheres that were believed best kept as distinct from one another as possible. Foremost among these are national jurisdictions, demarcating national sovereignties. The Bush administration has actively and aggressively moved in numerous ways since 9/11 to extend its surveillance and its coercive reach across national boundaries, to the extent that

many of its allies have become increasingly resentful.

Of more immediate concern within the US is the concerted drive to break down various firewalls that have been maintained in the past to protect the private sector from government control. The tracking of those directly responsible for 9/11 – the biggest single criminal investigation in history – pointed to private sector databases (involving, for instance, credit card, telephone, and air miles data) for essential clues in reconstructing the trail of the terrorists. Money laundering investigations, involving reporting and automatic surveillance of a very wide range of private financial transactions, had already begun in relation to criminal activities, but since 9/11 have been greatly stepped up to track terrorist financing trails.

The appropriation of private sector data has proved very useful in the investigation of terrorist trails. But *post hoc* investigation is the least significant use of all-source data collection for counter terrorism. The major thrust is *risk profiling*, concerned not with the past, but with the future; less with who have already engaged in terrorist acts, but with who *might be* terrorists. Profiling is about risk calculation. The more information available, so the argument goes, the better is the likelihood of constructing accurate high risk categories and thus actionable profiles of potential terrorists. Breaking down the firewalls separating private data bases from public scrutiny is in this sense a necessary first step in terrorism prevention.

More subtly, a series of internal firewalls that had separated databanks held within government itself, have also fallen under attack. The most notable of these is the distinction between counterintelligence investigations of foreign espionage operations in America, and criminal law enforcement, with lower standards with regard to legal safeguards for the targets of surveillance in the former. In general, faced with borderless threats, government has sought to gain access to a seamless web of information on citizens and non-citizens drawing on all potential sources.

This thrust has plausible arguments in its favour, rooted in the specific nature of the terrorist threat, with a ready constituency among a fearful public. It is also important to point to the inherent dangers. There are very good reasons why the various firewalls have been erected around data collected for different purposes by different agents, and why restraints have been imposed historically on government access to personal information. The right to privacy has long been viewed as a fundamental element of a free society, but one that is increasingly in question in the era of new information technologies.

U.S. ANTI-TERRORIST SURVEILLANCE POWERS

Introduced within a week of the 9/11 attacks and rushed through Congress under great pressure, the USA PATRIOT Act was signed into law on October 26, 2001.[5] Its provisions significantly expand the electronic surveillance powers of federal law enforcement authorities, often without providing appropriate checks and balances to protect civil liberties. Ideas that had previously been put forward by the executive and subjected to strenuous criticism were whisked through the legislative process after 9/11.

With regard to communication surveillance, the Act relaxes restrictions around required warrants and court orders. It extends court orders to cover e-mail messages and internet use, and extends court orders to cover the entire US, as opposed to being limited to the judicial district in which the court has jurisdiction as in the past. Critics point out that, even though the capture of message content is specifically prohibited, e-mail header information, which may include subject headings, or the addresses of specific web sites visited, may be much more revealing than the simple telephone numbers previously captured.

This provision may provide sanction to the FBI's CARNIVORE program, even though once installed by an internet service provider, CARNIVORE may monitor all the communications of all subscribers, not just those targeted by a court order.[6] Although the Act imposes no positive obligation on service providers to modify their systems to accommodate law enforcement needs, anecdotal information suggests that after 9/11, internet service providers have come under increasing pressure to assist, even in the absence of specific court orders.[7] However, to what extent providers have installed CARNIVORE is not known, since public disclosure of such information is prohibited.

The Act lowers the barriers between criminal investigations and foreign intelligence information. Facilitating closer cooperation between criminal investigators and foreign intelligence collectors is probably not a controversial intention in itself, but more debatable is the extension to criminal investigations of the much laxer standards of protection required under the Foreign Intelligence Surveillance Act (FISA) is debatable. FISA was originally a response to concerns about domestic spying that surfaced during the 1970s. While the need for special surveillance powers and secret evidence in relation to foreign espionage activities in the US was widely accepted, it was generally believed that such methods were unacceptable against American citizens, especially those engaged in First Amendment free speech, as with the Vietnam War protests. Under FISA, government operates on a

lower threshold for gaining authorization for intrusive surveillance against targets suspected of espionage and foreign intelligence operations in the USA than is the case for criminal investigations. For instance, under FISA, investigators gain access to records from car rental agencies, motel accommodations, and storage facilities, as well as easier recourse to physical searches and wiretaps. Special FISA courts meet *in camera*, with non-disclosure of evidence deemed to be of a sensitive intelligence nature.

Under the PATRIOT Act, FISA is amended in certain crucial and significant ways. If evidence of a criminal offence was uncovered from FISA surveillance, prosecution could not be based on FISA surveillance, but would have to be based on a surveillance order under a narrower and more restrictive authorization for wiretap orders. Now foreign intelligence gathering need only be a "*significant* purpose" to trigger a FISA surveillance or search order. This compromise departs significantly from the clear distinction originally drawn between surveillance for criminal law enforcement, and surveillance for foreign intelligence. for the lower threshold.

Not content with lowering the threshold, the PATRIOT Act widens FISA's powers. It permits 'roving surveillance', that is, orders that are not tied to a particular place or particular means of communication. While it is not unreasonable to point out that those seeking to evade surveillance will constantly shift their means and location of communication, there are obvious dangers that roving surveillance will capture communications among persons not named in the order. The Act extends FISA to cover e-mail as well as telephone communication. It extends the duration of surveillance and physical search orders, in some case providing extensions of up to a year.

Questions about how government would use expanded access to FISA orders were raised in 2002 when the FISA court itself issued a stunning rebuke to the Justice Department,[8] identifying more than 75 cases in which it says it was misled by the FBI in documents in which the bureau attempted to justify its need for wiretaps and other electronic surveillance. The F.B.I. and the Justice Department were said to have violated the law by allowing information gathered from intelligence eavesdrops to be used freely in bringing criminal charges, without court review, and criminal investigators were improperly directing the use of counterintelligence wiretaps. In August 2002, the Justice Department appealed this opinion to the little known Foreign Intelligence Surveillance Court Of Review, arguing that the USA PATRIOT Act now permitted FISA to be used to obtain evidence for a prosecution if the government also has a significant non-law enforcement foreign intelligence purpose.[9]

On November 18, the Review Court, in its first ever decision, concluded that FISA, as amended by the PATRIOT Act, supports the government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution."[10] "Proclaiming a major victory in the war on terrorism, Attorney General Ashcroft said the decision 'revolutionizes our ability to investigate and prosecute terrorists' because it permits criminal investigators and intelligence agents to work together and to share information."[11] The *New York Times* called the decision 'A Green Light to Spy'.[12] As if in confirmation, the Attorney General announced plans to intensify secret surveillance, including the designation of special intelligence prosecutors in every federal court district, and the creation of a new FBI unit to seek intelligence warrants.[13] In March 2003, Ashcroft revealed that he had personally authorized secret electronic surveillance and physical searches without court oversight in 170 'emergency' cases since the Sept. 11 attacks -- more than triple the emergency searches authorized by other attorneys general over the past 20 years.[14]

The final section of the PATRIOT Act that raises issues about privacy protection is the expanded authority of the Treasury Secretary to regulate and probe the activities of financial institutions, especially their relations with foreign entities, in pursuit of money laundering. US jurisdiction is extended to prosecute money laundering offences abroad. The most controversial aspect of the expanded surveillance powers in the Act is the concerted attempt to extend the cooperation of financial institutions, securities dealers and brokers, as well as commodity merchants, etc., with law enforcement agencies with regard to suspected terrorist associated money laundering. In effect, the Act seeks to enlist financial institutions as active participants in the government's surveillance program, yet another example of the tendency to break down barriers between the public and private sectors. Failure to cooperate actively could result in severe penalties, including seizure of assets.

Early in 2003, a draft version of a new and expanded PATRIOT Act was leaked to a public interest advocacy group. The Domestic Security Enhancement Act of 2003 would, among other things, prohibit disclosure of information regarding people detained as terrorist suspects; create a DNA database of "suspected terrorists"; place the onus on suspects to prove why they should be released on bail; and allow the deportation of U.S. citizens who become members of or help terrorist groups.[15]

Nor have the appetites of the executive and Congress for intrusive surveillance powers been exhausted by the language of the *PATRIOT Act*. The *Homeland Security Act*, signed by the President in November 2002, contains additional powers for electronic surveillance. It permits internet service providers voluntarily to provide government agents with access to the contents of their customers' private

communications without those persons' consent based on a "good faith" belief that an emergency justifies the release of that information. 20-year prison terms are provided for computer hackers..[16]

SURVEILLANCE IN PRACTICE

The Attorney General has released new investigative guidelines for the Justice Department reflecting its mission to "neutralize terrorists before they are able to strike", and to shift emphasis from criminal investigation to crime "prevention". Among these guidelines is authorization given to the FBI to conduct "online research" for counterterrorism purposes, "even when not linked to an individual criminal investigation". Moreover, the FBI is authorized to use "commercial data mining services to detect and prevent terrorist attacks, independent of particular criminal investigations". The FBI is further enabled to establish its own databases drawn from multiple sources, and to operate "counterterrorism information systems."[17]

One of the surveillance spinoffs from the PATRIOT Act that has come to partial notice is its application to libraries and bookstores. FISA court orders, now extended to e-mail on online communication, apparently include records of URLs visited in web surfing, or the detailed information such as keywords recorded in search engines consulted online. Persons seeking anonymity in internet use may use library online facilities. Libraries have consequently been visited by the FBI seeking records of usage and identification of users, citing 'roving' warrants. The FBI may also have sought to have their surveillance software, like CARNIVORE, installed on library systems. Libraries and bookstores may be required to provide records of books borrowed, or purchased, by persons under suspicion. The incidence of such requests, and the degree of compliance, is not known: Catch-22 is that the FBI prohibits disclosure regarding such orders. This has led one commentator to suggest that Attorney General Ashcroft may have been reading Kafka in his local library.[18] This is uncomfortably reminiscent of the notorious FBI 'Library Awareness Program' that from the 1960s to the late 1980s attempted to bully librarians into snooping into the reading habits of patrons deemed left-wing or anti-American by the FBI.[19] Could we now be seeing attempts to track and identify persons reading about Islam or terrorism?

This raises another serious problem in evaluating the impact of the new powers: the administration is resistant to providing Congress access to information on the implementation of the Act. Congress, which was pressured into passing the USA PATRIOT Act without due deliberation, did add sunset clauses to

many key sections, under which authority is terminated by Dec. 31, 2005, unless extended by Congress. If sunset provisions are to have any real force, Congress must have access to sufficient information to make informed judgments on whether the extension of new powers is justified. Yet when a bipartisan request was made by Congress in July 2002 that a wide range of questions concerning the implementation of the PATRIOT Act be answered by the executive, the government failed to respond to most of their questions. Even threats of subpoenas have not succeeded in dislodging much more information.

There are plausible arguments in favour of secrecy when issues of security against terrorist attack are at stake. But most of the critics of government stonewalling do not challenge the reasonableness of keeping genuinely sensitive and potentially damaging information out of the public realm. Their expectations are simply for a level of information that will permit democratic accountability, and allow the public informed judgments on government's performance in the war on terrorism. The excessive secrecy and the active resistance to requests for information, even from the legislative branch, follow a familiar pattern of governments with authoritarian tendencies: as they expand their intrusive gaze into the interstices of private life, they seek to render their own actions opaque to the citizenry. This was the precisely the role of the Inspector in Bentham's Panopticon, his design for a prison that serves as the paradigm for all modern surveillance.[20] Yet in the contemporary world of de-centred, multidirectional surveillance, attempts to prevent the watched from watching their watchers are doomed to limited success in practice. Technologies of surveillance are so widely diffused, and so cheaply deployed, that the state's attempts to shroud its own actions in secrecy inevitably fall under criticism, and even ridicule. Since 9/11, the balance in public access to government information has undoubtedly shifted toward non-disclosure, but government actions are too exposed to everyday publicity to escape the scrutiny of critics. Some of the most ambitious US government surveillance projects, as we shall see, have been exposed to such withering public derision that they have had to be retracted or severely curtailed.

TOWARD 'TOTAL INFORMATION AWARENESS'?

The first surveillance project to overstep the invisible line between public tolerance and outrage was the Justice Department's ill-starred TIPS program. TIPS (Terrorism Information and Prevention System)

envisioned mobilizing a volunteer army of informants for the “stated purpose of creating a national information sharing system for specific industry groups to report suspicious, publicly observable activity that could be related to terrorism.”[21] Certain occupations that provided access to private homes, such as utilities personnel, letter carriers, cable and telephone repair people, were identified as particularly useful sources, but a national TIPS hotline was also established for concerned private citizens to report suspicions about neighbours or local happenings to a central FBI data bank. Reaction was immediate and vociferous. Ashcroft’s idea was likened to the infamous Stasi secret police in the former East Germany. Other critics pointed out that the FBI did not need the task of sifting through neighbourhood gossip while trying to track global terrorist threats. Exposed to a mixture of indignation and ridicule, TIPS was first scaled back, and then withdrawn altogether, vanishing from government websites as if it had never existed.[22]

TIPS was an old-fashioned, low-tech, prosaic surveillance project that was understandable enough to be widely recognized as unacceptable in a free society. Another project, that defines itself by its cutting-edge technology, and was conceived in expansive, global, terms, has also been met with fierce resistance. This goes under the Orwellian title of ‘Total Information Awareness’ (TIA).’

The true visionary for a post-9/11 global surveillance state is neither John Ashcroft, nor the directors of any of the existing security and intelligence agencies. Instead he is Vice Admiral John M. Poindexter, of Iran-Contra affair notoriety. Admiral Poindexter, whose conviction for lying to Congress was reversed in 1991 by a federal appeals court because he had been granted immunity for his testimony, has been rehabilitated by the Bush administration and made Director of the Information Awareness Office in the Defence Advanced Research Projects Agency (DARPA). DARPA has a distinguished lineage in the information age. It was from this office that the Internet sprang. In 1969 DARPA set up a pioneer computer network among defence scientists called ARPANET, which after a series of transformations, and freed of its original sponsor, eventually evolved into the Internet.[23] DARPA has a mandate to develop and apply new surveillance technologies post-9/11.

The concept of ‘Total Information Awareness’ was initially revealed to the world on a website featuring a logo of a large eye atop a pyramid scanning the globe, under the slogan ‘*scientia est potentia*’ (knowledge is power). Poindexter’s office was putting together a series of research teams working on advanced surveillance technologies of various kinds, from bio-recognition technologies to sophisticated translation systems to bio-surveillance providing early warning of attacks of biological agents. He envisaged a cutting-edge system for detecting, classifying, identifying, and tracking terrorists.

He wished to “punch holes in the stovepipes” that separate different data collections and develop a seamless global system that mines data from all possible sources, public and private, American and foreign. One of the “significant new data sources that needs to be mined to discover and track terrorists is the *transaction space*.” Terrorists move easily under cover, but they leave an “information signature. We must be able to pick this signal out of the noise.”[24]

The *Washington Post* editorialized that “anyone who deliberately set out to invent a government program with the specific aim of terrifying the Orwell-reading public could hardly have improved on the Information Awareness Office.”[25] The archconservative *New York Times* columnist William Safire, usually a strong Republican supporter, denounced this “supersnoop's dream”.[26] The very idea of such a global intelligence system – tracking the ‘transaction space’ within the US as well as around the globe – set off alarm bells from all quarters and all sides of the political spectrum about Big Brother and the end of privacy. Critics pointed out that privacy laws and regulations in the US (not to speak of Europe and Canada, where extraterritorial invasions of privacy would be certain to rouse opposition) could not be blithely and unconstitutionally set aside by Washington simply by invoking national security. The administration began backtracking, and the TIA website began bit by bit to vanish, beginning with the sinister logo and the motto, followed by the laundered biography of Admiral Poindexter as well as the biographies of his senior associates, along with graphics depicting the sweeping global ambitions of the program. Eventually the site has been modestly re-titled ‘Information Awareness Office’, and contains numerous assurances that nothing contemplated by the TIA program will overstep privacy protections. [27] Bipartisan agreement in Congress supported an amendment to hold up funding for TIA until the administration explained it in detail to Congress, including its impact on civil liberties, and to bar any deployment of the technology against US citizens without prior Congressional approval, but no controls over its deployment abroad.[28]

Qualms about constitutionality and privacy aside, it must be admitted that a program such as TIA fits rather easily into the technological and economic realities of the early 21st century. As one newspaper report put it, “it is increasingly possible to amass Big Brother-like surveillance powers through Little Brother means. The basic components include everyday digital technologies like e-mail, online shopping and travel booking, A.T.M. systems, cellphone networks, electronic toll-collection systems and credit-card payment terminals.”[29] TIA simply looks toward developing software that can put all this diffuse private and public data together in ways that will flag suspicious behaviour patterns for attention. Nor have Congressional roadblocks discouraged the US government from floating TIA-like schemes under other names and other auspices. A new Terrorist Threat Integration Center (TTIC), will begin work in

May 2003 combining the resources of the CIA and the FBI to analyze foreign and domestic intelligence collected throughout the government to better "connect the dots" and prevent future terrorist attacks. The center, according to the White House, "will have unfettered access to all terrorist threat intelligence information, from raw reports to finished analytic assessments, available to the U.S. government."[30] The Transportation Security Agency recently announced that the Computer Assisted Passenger Pre-screening System II (CAPPS II) will begin testing at several airports around the U.S. starting sometime in March. CAPPS II is a system for conducting background checks on all airline passengers and categorizing them according to level of risk they pose. The ACLU warns that "CAPPS II is based on the same concept as the Pentagon's 'Total Information Awareness' program, which proposed massive fishing expeditions through some of our most personally sensitive data."[31]

Serious questions arise about the justification for TIA-type programs even in terms of their own stated objectives. There is a consensus among informed experts that the 'intelligence failure' of 9/11 is attributable less to a collection deficit than to an *analytical* deficit. There were many bits and pieces of information concerning the threat from Al Qaida, and even the imminence of a major attack on American soil. The key failing of the intelligence community was its inability to put the pieces together and make sense of the bigger picture. It has been widely observed in the US and elsewhere that as a general rule, the collection capacity of intelligence agencies has outstripped their analytical capacities. TIA-type schemes actually threaten to worsen this imbalance, swamping overworked analysts with too much information, almost all of it irrelevant, but requiring processing. The idea that out of a deluge of detailed information from banking, credit, debit, air miles, and other data bases, actionable profiles of potential terrorists will somehow emerge is more a matter of faith than of science (not perhaps entirely unlike the touching faith in computers and American know-how that fuels the scientifically dubious scheme for a fail-safe anti-missile shield).

It is possible to become over-alarmed about the Orwellian prospect, especially if one accepts too readily the techno-hype behind it. The intentions may be alarming, but the means of delivering TIA are as yet more suspect than enthusiasts like Admiral Poindexter believe. There are questions surrounding many of the technologies that are being promoted by the private sector to the US government as quick fixes for terrorism. When the Defense Department tested face-matching technologies, their results were less impressive than the figures claimed by the companies peddling them.

There are also some important technological limitations on Big Brother's surveillance capacities. Chief among these is the universal accessibility of encryption systems that defeat the decryption capabilities of

the NSA and all other intelligence agencies, American or foreign. Government snoopers are by and large resigned to living with an inability to read intercepted e-mail messages.[32] The UK government, prior to 9/11, went so far as to legislate criminal sanctions for persons who refuse to disclose their encryption keys to police or security officials who demand them, but the US government has declined to follow this example. The reason for US reticence is not hard to find: opposition to the British legislation came not only from civil libertarians, but more influentially, from e-commerce interests irritated at government intrusion into security systems, the integrity of which is essential to e-commerce transactions.

This points to an inherent contradiction in the relations between public and private actors as barriers between state and corporate surveillance systems are lowered. There are two very different, and sometimes antagonistic, concepts of 'security' at work. To the public sector, security comes from accessing and controlling the 'transaction space'. To the private sector, security means guaranteeing the integrity of transactions with clients, whether consumers or other businesses. In the face of the terrorist threat as embodied in 9/11, there is good reason for business to buy into government surveillance programs to make their own operations more secure – indeed, there is a lot of money to made by private companies in equipping government surveillance operations. Yet the corporations are not always on the same page as government, or indeed on the same page as each other. These confusions lead to a peculiar, stuttering dynamic in the development of government surveillance programs.

Actually, the contradictions are even more acute. The vulnerabilities of private sector security are hyped and indeed over-hyped by the private security industry that has a vested interest in advancing sales of its software and hardware systems. The very notion of cyberterrorism has been characterized as overblown and alarmist.[33] Dire predictions of an 'electronic Pearl Harbor' almost certainly run ahead of the actual potential for damage. Many critical infrastructures, such as air traffic control and power systems, communicate within 'intranets', not connected to the internet, and are 'air-gapped' to provide protection from malicious hackers cruising the net looking for targets. Yet alleged vulnerabilities are deliberately exaggerated by those with security systems to sell credulous government officials. Government is thus being pushed in different directions by different private interests, at the same time as it extends its surveillance of the private sector.

A SECURITY-INDUSTRIAL COMPLEX

To assess the impact of 9/11 and the future direction of the surveillance state, it is necessary to look at

the relations of government with the private sector, or more precisely, with various private sectors. The Bush administration has sought to dramatically extend its surveillance reach as a counter-terrorist strategy. In doing so, it has constructed close links with certain corporate interests in the high-tech, dot.com sector. Homeland security is quickly shaping up as the biggest government contract bonanza since the end of the Cold War. If President Eisenhower warned in his farewell address in 1961 of a military-industrial complex, the war on terrorism has generated an emergent security-industrial complex.[34] Homeland Security secretary Tom Ridge has been an enthusiastic advocate of public-private partnership: "We look to American creativity to help solve our problems and to help make a profit in the process."[35] Tens of billions of dollars are on the table, and are being snapped up by companies that, like the Cold War defence industries, have in the first instance a single customer, Uncle Sam. This has been a godsend for a sector recovering from the huge hit of the dot.com collapse prior to 9/11. Their profitability rests on a continued market in government for new surveillance and security technologies, and on the hope for commercial spinoffs as business and society look for technological security fixes. In both cases, the security-industrial complex has a stake in joining with government in pumping up the threat level, just as the defence interests and the government pumped up anxiety over the Soviet threat in the past – including 'missile gaps' that never were.

This is the complex context in which the Bush administration's efforts to amass new and intrusive surveillance powers must be assessed. In the end, it may well be that privacy protection laws, resistance by both civil libertarians and sections of the private sector, as well as over reliance on technology, may ensure that the administration's reach exceeds its grasp.

THE FAUSTIAN BARGAIN

Despite obstacles and setbacks, the concept of TIA is by no means discredited within US government circles. Data-mining, or dataveillance, under government direction in the name of fighting terrorism, is an idea whose time has clearly arrived. Implicit in this is the concept of a global surveillance regime. Since the terrorist threat knows no boundaries. exempting Americans from the panoptic gaze makes little sense. Nor can walls erected between private and public data sources be functionally justified, especially when the private sector rushes to offer its troves of personal data to government in the name of patriotism and public spirit, which has been happening frequently since 9/11.[36] The full blown, original manifestation of TIA, before its emasculation, suggests much more than mere bureaucratic or

technocratic response to the challenge of terrorism. *Scientia est potenta* is a motto fraught with significance. The idea that knowledge is power was a driving force of the 20th century, fuelling the huge state investments in science and technology, and the mobilization of science in wars and cold wars, as well as the hyper development of intelligence gathering to steal the knowledge of other states (the history of nuclear weaponry is emblematic). In the 21st century, the information technology revolution has proceeded much more importantly in the private than in the public sector. But the Promethean possibilities of harnessing the vast information resources diffused throughout the de-centred, multiple surveillance systems around the globe are, to those on the commanding heights of an American state that is unchallenged as the globe's only remaining superpower, too tantalizing to pass by.

Nor is it any accident that the TIA concept arose within the US Department of Defense. The dominant military philosophy that drives American military power and interventions in the 21st century derives from the 'revolution in military affairs' that has produced 'network centric warfare'. Information and control over information is key to this concept, in which intelligence guides the organization of the 'battlespace', and the delivery of devastating and sophisticated weaponry with a degree of precision never seen before. The enemy's communications infrastructure will be targeted in the first wave of attack, rendering the adversary 'blind' and 'deaf', while the attacker 'sees' and 'hears' everywhere. Clausewitz's famous 'fog of war', and his dictum that all military action is undertaken in a 'resistant medium' are now considered passé, obsolete wisdom from an earlier age, before penetrative surveillance and global positioning systems can be employed to see through the fog. The rapid collapse of the Taliban regime in the face of American intervention is seen as a preview of this new kind of warfare, and a token of its potential effectiveness. The American invasion of Iraq will be the first full-scale test case of the new warfare system. The evangelists of the new doctrine, firmly in command of the Defense Department and the Bush White House, are supremely confident that American military might (today equal to half the military force of the rest of the world's states combined) combined with unparalleled American intelligence capacity, can control any 'battlespace' the US chooses to engage, with minimal, acceptable levels of casualties, and that US economic resources will be equal to the challenge of financing this global military hegemony.[37]

It is in this context that we must view the pronounced turn of the Bush administration toward unilateralism in foreign policy – abrogation of the Anti-Ballistic Missile Treaty; renunciation of the chemical and biological weapons verification protocol; non-compliance with the Kyoto Accord; insistence on American exemption from the International Criminal Court; the invasion of Iraq without UN sanction, etc. – and the Bush Doctrine claiming the right to initiate preventive war by intervening

against any state that poses a real or potential threat to US security, as determined by the US alone. The present administration believes that building multilateral alliances and coalitions in support of US objectives is desirable, where possible, and so long as these do not interfere with American goals and timetables, but ultimately unnecessary, and dispensable. Hence the breakdown in the Western Alliance over Iraq, and even the possible marginalization into irrelevance of the United Nations, is viewed with apparent equanimity as a small price to pay in exchange for the opportunity to redraw the geopolitical map of the Middle East on American terms.

This is the setting in which the concept of TIA has to be understood. Particular programs, and particular personnel, may suffer setbacks and rebukes from Congress, commentators, and the public, but there is an underlying logic and thrust that is highly unlikely to be displaced by civil libertarian scruples. TIA fits comfortably within the dominant strategic doctrine of Bush's America. Examining the prospectus offered by the enthusiasts of TIA, its language, its imagery, its moral, if not moralistic, tone, suggests strongly that there are more than technocratic practicalities involved. It is as if America has been offered a Faustian bargain by the promise of technology.

Look down from the heights, Mephistopheles tells Faust, and see the world at your feet, rendered transparent to your gaze, all secrets uncovered. Your enemies, real and potential, will speak to you henceforth in the voice of Psalm 139:

Such knowledge is too wonderful for me;

It is high, I cannot attain unto it….

If I say, Surely the darkness shall cover me;

Even the night shall be light about me.

Yea, the darkness hides not from thee;

But the night shines as the day:

The darkness and the light are both alike to thee.

All this is yours, promises the voice of technological power. There will, of course, be the small matter of a *quid pro quo*: at the end of the day, you will have to abandon your constitutional protection of human rights, to the extent that these get in the way. These are regrettable, but Faust reflects that "the other side weighs little on my mind" compared to the new world rising before his eyes – "The rest concerns me not: Let come what will."[38]

What Faust forgets is an earlier exchange with Mephistopheles, when he has interrogated the latter about his "all-knowing wit". The Prince of Darkness demurs, slightly: "Omniscient? No, not I; but well-informed." Undoubtedly, the vast surveillance powers available to the US can make that country's government better informed, but to reach for *omniscience*, even as a distant but attainable goal, is to fly in the face of the limitations of the political economy of the technology itself, as well as the capacity of analysts, however intelligent, objective, and well-intentioned (and these are not, by and large, the qualities that spring to mind in describing those currently in charge of the US administration), to give meaning to the relentless, bottomless, ocean of 'facts' they can now conjure up. Total Information Awareness is a concept that suggests, more than anything else, *hubris* – the same quality that so much of the world today sees in American foreign and defence policy in general.

It may also be the wrong answer to the right question. If neo-liberal globalization has re-created the old Hobbesian problem of insecurity and disorder, this time on a world scale, it may well be necessary to look for Hobbesian solutions. In 17th century England, the effects of the rising market on society had suggested to Hobbes that, without government, life would resemble a 'war of all against all'. The micro-rationality of individuals pursuing their self-interest resulted in the macro-irrationality of a world in which life was "solitary, poor, nasty, brutish, and short". His answer derived from enlightened self-interest: each person would transfer their power to the Sovereign, the Leviathan state, which would in turn guarantee the security of all.

Today, the dark side of globalization threatens the security of the world of Leviathan states that has, since Hobbes' day, internationalized the market. When the terrorists struck at the World Trade Center, symbol of global commerce, they simultaneously challenged the global order, and challenged the US state, which failed in its fundamental Hobbesian task of protecting its own citizens. The US resolved to put an end to the threat of disorder posed by the terrorists, and, in this resolve, were supported by most of the world's states, and peoples. Certainly, American leadership and initiative is both necessary, and welcomed by all who share the insecurity posed by the terrorist threat. The *hubris* of America is shown, not in this resolve for leadership, but in America's pretension in itself assuming the role of the new

global Leviathan.

The terrorist networks, like the wider forces of the dark side of globalization, pose borderless threats, operating in the new global space of flows, leaving the territorially bounded legal and policing jurisdictions of national states largely impotent to control them. Global governance requires enforcement, but only national states possess effective enforcement powers. A 21st century Hobbesian answer to global disorder is the Multilateral Leviathan – a broad alliance or network of states cooperatively coordinating their enforcement powers to contain and limit borderless threats that make each of them insecure, according to multilateral agreements and treaties, with international sanction. American leadership would have been at the heart of any such Multilateral Leviathan, but coalition building on this scale requires tact, diplomacy, the arts of compromise and negotiation, and a willingness to listen and learn from others – all qualities in notoriously short supply, if not entirely absent, from the Bush White House. As the president declared in the wake of 9/11: "You are either with us, or on the side of the terrorists." *With us*, it now appears to much of the world, means *under us*. The impressive global coalition of support assembled for the Afghanistan intervention has shrunk desperately for Iraq. The Americans speak of a 'coalition of the willing' but what most of the rest of the world sees is a coalition of the bribed, the bullied, and the bilked.

Total Information Awareness, either as a program or a concept, represents overreach. It is a symbol of a greater *hubris* that threatens in the longer run to bring down America's plan to assume the role of a global but unilateral, Leviathan.

---

[1] Reg Whitaker, *The End of Privacy: How Total Surveillance is Becoming a Reality* (NY: New Press, 1999).

[2] United States Department of the Treasury, Financial Crimes Enforcement Network, *Strategic Plan 2000-2005*

[3] Simon Davies, ‘Spies like US’. *Daily Telegraph,* 16 December 1997

[4] Astonishingly, in two cases of suspected terrorists who hold American citizenship (José Padilla and Yaser Esam Hamdi), the Justice Department has repeatedly asserted a claim that their constitutional protections can be set aside, and that the government’s decisions must not be subject to review by the judicial branch. So far the Justice Department has at least partially avoided adverse court rulings in these cases.

[5] P.L. 107-56, 115 Stat. 272 (2001), Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism (USA PATRIOT ACT)

[6] An internal FBI e-mail message dated April5, 200 recounts how a pre-9/11 investigation of terrorists linked to Osama bin Laden went awry when CARNIVORE captured not only the communications of the court-authorized target, but also picked up e-mails of non-covered individuals, in violation of federal wiretap law: ‘FBI Docs Obtained by EPIC: Carnivore Hampered Terror Probe’, EPIC Alert 9/11 June 5, 2002.

[7] Declan McCullagh, ‘Anti-Attack Feds Push Carnivore’, *Wired News* Sept. 12, 2001, reported that “Just hours after three airplanes smashed into the buildings…FBI agents began to visit Web-based, e-mail firms and network providers, according to engineers at those companies who spoke on condition of anonymity…An administrator at one major network service provider said that FBI agents showed up at his workplace on Tuesday "with a couple of Carnivores, requesting permission to place them in our core, along with offers to actually pay for circuits and costs."

[8] US Foreign Intelligence Surveillance Court, Memorandum Opinion, May 17, 2002, available at: http://www.washingtonpost.com/wp-srv/onpolitics/transcripts/fisa_opinion.pdf. Philip Shenon, ‘Secret Court Says F.B.I. Aides Misled Judges in 75 Cases’, *New York Times,* August 23, 2002; Dan Eggen and Susan Schmidt, ‘Secret Court Rebuffs Ashcroft: Justice Dept. Chided On Misinformation’, *Washington Post,* August 23, 2002

[9] Philip Shenon, 'Justice Dept. Denounces Secret Court on Wiretaps' *New York Times*, September 28, 2002

[10] United States Foreign Intelligence Surveillance Court Of Review: In re: Sealed Case No. 02-001 Consolidated with 02-002, On Motions for Review of Orders of the United States Foreign Intelligence Surveillance Court (Nos. 02-662 and 02-968). Argued September 9, 2002, Decided November 18, 2002

[11] David G. Savage and Henry Weinstein, 'Court Widens Wiretapping in Terror Cases', *Los Angeles Times*, November 19 2002

[12] *New York Times*, editorial: 'A Green Light to Spy', November 19, 2002

[13] Dan Eggen, 'Broad U.S. Wiretap Powers Upheld', *Washington Post*, November 19, 2002, p. A01

[14] Richard B. Schmitt, **'**U.S. Expands Clandestine Surveillance Operations**''**, *Los Angeles Times* , March 5, 2003

[15] The Center for Public Integrity, Justice Dept. Drafts Sweeping Expansion of Anti-Terrorism Act: http://www.publicintegrity.org/dtaweb/report.asp?ReportID=502&L1=10&L2=10&L3=0&L4=0&L5=0; Curt Anderson, 'Expansion of Patriot Act Criticized', *Associated Press*, 8 February 2003.

[16] Electronic Privacy Information Center (EPIC), *Alert*, 9:23, November 19, 2002

[17] *Ibid*, pp.26-28

[18] Mary Minow, 'The USA PATRIOT Act and patron privacy on library internet terminals'. LLRX. Com, February 15 2002', http://www.llrx.com/features/usapatriotact.htm. Nat Hentoff, 'Has the Attorney General Been Reading Franz Kafka?', Village Voice, February 9, 2002. Martin Kasindorf, 'FBI's reading list worries librarians', *USA Today*, Dec. 17, 2002.

[19] Herbert N. Foerstel, *Surveillance in the Stacks: The FBI's Library Awareness Program* (Westport, Conn.: Greenwood Press, 1991)

[20] Jeremy Bentham, *The Panopticon Writings*, Miran Božovl, ed. (Lonodn: Verso, 1995)

Michel Foucault, *Surveiller et punir: naissance de la prison* (Paris: Gallimard, 1975)

[21] 'Operation Tips Fact Sheet' from the Justice Department website, summer 2002. For reasons that will be made clear, all TIPS information later disappeared from this and other US government websites. The only remaining records are those now archived by independent observers, and media accounts at the time.

[22] Dan Eggen, 'Proposal to Enlist Citizen Spies Was Doomed From Start', *Washington Post*, November 24, 2002; Page A11

[23] Manuel Castells, *the Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford: Oxford University Press, 2001) pp. 10-29

[24] Dr. John Poindexter, Director, Information Awareness Office of DARPA, 'Overview Of The Information Awareness Office', Remarks as prepared for delivery by, at DARPATech 2002 Conference, Anaheim, Calif., August 2, 2002, http://www.fas.org/irp/agency/dod/poindexter.html. See also John

Markoff, ‘Pentagon Plans a Computer System That Would Peek at Personal Data of Americans’, *New York Times*, November 9, 2002; Robert O'Harrow Jr., ‘U.S. Hopes to Check Computers Globally: System Would Be Used to Hunt Terrorists’, *Washington Post*, November 12, 2002; Page A04

[25] ‘Total Information Awareness’, *Washington* Post, November 16, 2002; Page A20

[26] William Safire, ‘You Are a Suspect’, *New York Times*, November 14, 2002

[27] http://www.darpa.mil/iao/news.htm

[28] Adam Clymer, ‘Conferees in Congress Bar Using a Pentagon Project on Americans’, *New York Times*, February 12, 2003; William Safire, ‘Privacy Invasion Curtailed’, *New York Times*, February 13, 2003

[29] John Markoff And John Schwartz, ‘Many Tools of Big Brother Are Up and Running’, *New York Times*, December 23, 2002

[30] Curt Anderson, ‘Bush Announces New Counterterrorism Center’, *Associated Press*, February 14, 2003

[31] ACLU, ‘CAPPS II Data-Mining System Will Invade Privacy and Create Government Blacklist of Americans’, February 27, 2003: http://www.aclu.org/Privacy/Privacy.cfm?ID=11956&c=130; ‘The new airport profiling’, *New York Times*, March 11, 2003.

[32] There are also sophisticated encryption systems for hiding messages in the digital coding for pictures, or sound messages, that are even more difficult to flag as suspicious, let alone decipher.

[33] Joshua Green, 'The myth of cyberterrorism', *Washington Monthly* (November 2002); James A, Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, DC: Center for Strategic & International Studies, December 2002)

[34] Brendan I. Koerner, 'The security traders', *Mother Jones* (September-October 2002)

[35] Alison Mitchell, 'Industry Sees Opportunity in U.S. quest for Security', *New York Times*, November 25, 2001

[36] For example, it was recently revealed that eBay, the largest online retailer in the world, voluntarily provides all its data on its customers to law enforcement officials on request. Yuval Dror, 'Big Brother is watching you - and documenting', *Ha'aretz* English language edition, 20 February 2003.

[37] Gregory J. Walters, *Human Rights in an Information Age: a Philosophical Analysis* (Toronto: University of Toronto Press, 2001) 187-237, has assessed the concept of 'information warfare' from the ethical perspective of human rights.

[38] Quotations from Goethe, *Faust*, translated by Philip Wayne (Harmondsworth: Penguin, 1949)

September 11, 2001, is a day that shaped history and impacted the world for generations to come. From news coverage to strengthened airport security, here's how the world changed after the 9/11 attacks.Â One of the most persistent effects of the 9/11 attacks has been the ongoing war in Afghanistan. Shortly after the attacks, the United States under President George W. Bush began bombing Afghanistan. Because the Taliban-run government refused to give up suspected terrorist leader Osama Bin Laden, the United States began bombing the country in October. His brother Geoff, it transpired over the next few agonising hours, was in the World Trade Centre. "My mother had just flown out the day before to join us for a week," he remembers. "I recall being on the beach and I think my wife had gone up to one of the restaurants to get some food.Â Any apparent discrepancy was cleared up by a 2008 report by the National Institute of Standards and Technology (NIST) which found that WTC7 collapsed after fires on multiple floors "caused a critical support column to fail, initiating a fire-induced progressive collapse that brought the building down". The Big Brother conspiracy is Big government being or acting as a Totalitarian State, whether its subjects realize it or not. The name Big Brother comes from a character in George Orwell's Nineteen Eighty-Four. He is both the eyes and the voice of the political leader of the Totalitarian State in which the main character Winston Smith lives. The term has been applied to modern governments, predominantly democratic. As surveillance technology grows more complex, it outpaces public understanding of the threats it poses. The future of surveillance looks far more expansive and invasive than the Big Brother metaphor can capture. Where weâ€™re headed, weâ€™re going to need better metaphors â€” ones that accurately capture the diffuse, discriminatory and often secretive nature of both government and private surveillance.Â In â€œ1984,â€ Big Brother never actually appears. Rather, he is the figurehead of a totalitarian political party that tries to break citizens of their free will, partly through warnings of persistent surveillance. â€œBig Brother is watching youâ€ goes the (sinister) refrain. While chilling, this doesnâ€™t quite capture what weâ€™re up against today.