# Who's in Big Brother's Database?

By James Bamford

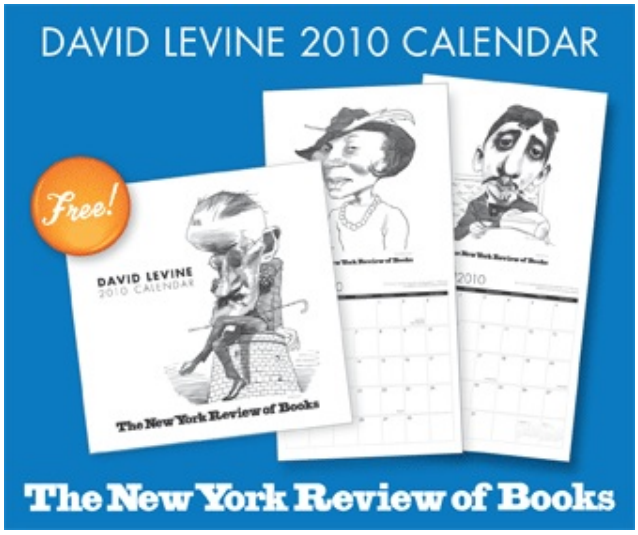
**The Secret Sentry: The Untold History of the National Security Agency**
**by Matthew M. Aid**

Bloomsbury, 423 pp., $30.00

On a remote edge of Utah's dry and arid high desert, where temperatures often zoom past 100 degrees, hard-hatted construction workers with top-secret clearances are preparing to build what may become America's equivalent of Jorge Luis Borges's "Library of Babel," a place where the collection of information is both infinite and at the same time monstrous, where the entire world's knowledge is stored, but not a single word is understood. At a million square feet, the mammoth $2 billion structure will be one-third larger than the US Capitol and will use the same amount of energy as every house in Salt Lake City combined.

Unlike Borges's "labyrinth of letters," this library expects few visitors. It's being built by the ultra-secret National Security Agency—which is primarily responsible for "signals intelligence," the collection and analysis of various forms of communication—to house trillions of phone calls, e-mail messages, and data trails: Web searches, parking receipts, bookstore visits, and other digital "pocket litter." Lacking adequate space and power at its city-sized Fort Meade, Maryland, headquarters, the NSA is also completing work on another data archive, this one in San Antonio, Texas, which will be nearly the size of the Alamodome.

Just how much information will be stored in these windowless cybertemples? A clue comes from a recent report prepared by the MITRE Corporation, a Pentagon think tank. "As the sensors associated with the various surveillance missions improve," says the report, referring to a variety of technical collection methods, "the data volumes are increasing with a projection that sensor data volume could potentially increase to the level of Yottabytes ($10^{24}$ Bytes) by 2015."[1] Roughly equal to about a septillion (1,000,000,000,000,000,000,000,000) pages of text, numbers beyond Yottabytes haven't yet been named. Once vacuumed up and stored in these near-infinite "libraries," the data are then analyzed by powerful infoweapons, supercomputers running complex algorithmic programs, to determine who among us may be—or may one day become—a terrorist. In the NSA's world of automated surveillance on steroids, every bit has a history and every keystroke tells a story.




In the near decade since September 11, the tectonic plates beneath the American intelligence community have undergone a seismic shift, knocking the director of the CIA from the top of the organizational chart and replacing him with the new director of national intelligence, a desk-bound espiocrat with a large staff but little else. Not only surviving the earthquake but emerging as the most powerful chief the spy world has ever known was the director of the NSA. He is in charge of an organization three times the size of the CIA and empowered in 2008 by Congress to spy on Americans to an unprecedented degree, despite public criticism of the Bush administration's use of the agency to conduct warrantless domestic surveillance as part of the "war on terror." The legislation also largely freed him of the nettlesome Foreign Intelligence Surveillance Court (FISA). And in another significant move, he was recently named to head the new Cyber Command, which also places him in charge of the nation's growing force of cyber warriors.

Wasting no time, the agency has launched a building boom, doubling the size of its headquarters, expanding its listening posts, and

constructing enormous data factories. One clue to the possible purpose of the highly secret megacenters comes from the agency's British partner, Government Communications Headquarters. Last year, the British government proposed the creation of an enormous government-run central database to store details on every phone call, e-mail, and Internet search made in the United Kingdom. Click a "send" key or push an "answer" button and the details of the communication end up, perhaps forever, in the government's data warehouse to be scrutinized and analyzed.

But when the plans were released by the UK government, there was an immediate outcry from both the press and the public, leading to the scrapping of the "big brother database," as it was called. In its place, however, the government came up with a new plan. Instead of one vast, centralized database, the telecom companies and Internet service providers would be required to maintain records of all details about people's phone, e-mail, and Web-browsing habits for a year and to permit the government access to them when asked. That has led again to public anger and to a protest by the London Internet Exchange, which represents more than 330 telecommunications firms. "We view...the volume of data the government now proposes [we] should collect and retain will be unprecedented, as is the overall level of intrusion into the privacy of citizenry," the group said in August.[2]

Unlike the British government, which, to its great credit, allowed public debate on the idea of a central data bank, the NSA obtained the full cooperation of much of the American telecom industry in utmost secrecy after September 11. For example, the agency built secret rooms in AT&T's major switching facilities where duplicate copies of all data are diverted, screened for key names and words by computers, and then transmitted on to the agency for analysis. Thus, these new centers in Utah, Texas, and possibly elsewhere will likely become the centralized repositories for the data intercepted by the NSA in America's version of the "big brother database" rejected by the British.

Matthew M. Aid has been after the NSA's secrets for a very long time. As a sergeant and Russian linguist in the NSA's Air Force branch, he was arrested and convicted in a court-martial, thrown into prison, and slapped with a bad conduct discharge for impersonating an officer and making off with a stash of NSA documents stamped Top Secret Codeword. He now prefers to obtain the NSA's secrets legally, through the front door of the National Archives. The result is *The Secret Sentry: The Untold History of the National Security Agency*, a footnote-heavy history told largely through declassified but heavily redacted NSA reports that have been slowly trickling out of the agency over the years. They are most informative in the World War II period but quickly taper off in substance during the cold war.

Aid begins his study on the eve of Pearl Harbor, a time when the entire American cryptologic force could fit into a small, half-empty community theater. But by war's end, it would take a football stadium to seat the 37,000 military and civilian "crippies." On August 14, 1945, as the ink dried on Japan's instruments of surrender, the linguists and codebreakers manning the thirty-seven key listening posts around the world were reading more than three hundred diplomatic code and cipher systems belonging to sixty countries. "The American signals intelligence empire stood at the zenith of its power and prestige," notes Aid. But within days, the cryptanalysts put away their well-sharpened pencils and the intercept operators hung up their earphones. By the end of December 1945, America's crypto world had shrunk to 7,500 men and women.

Despite the drastic layoffs, the small cadre of US and British codebreakers excelled against the new "main enemy," as Russia became known. The joint US-British effort deciphered tens of thousands of Russian army and navy messages during the mid-to-late 1940s. But on October 29, 1948, as President Truman was about to deliver a campaign speech in New York, the party was over. In what became known within the crypto world as "Black Friday," the Russian government and military flipped a switch and instantly converted to new, virtually unbreakable encryption systems and from vulnerable radio signals to buried cables. In the war between spies and machines, the spies won. The Soviets had managed to recruit William Weisband, a forty-year-old Russian linguist working for the US Army, who informed them of key cryptologic weaknesses the Americans were successfully exploiting. It was a blow from which the codebreakers would never recover. NSA historians called it "perhaps the most significant intelligence loss in US history."

In the 1970s, when some modest gains were made in penetrating the Russian systems, history would repeat itself and another American turncoat, this time Ronald Pelton, would again give away the US secrets. Since then, it has largely been a codemaker's market not only with regard to high-level Russian ciphers, but also those of other key countries, such as China and North Korea. On the other hand, the NSA has made significant progress against less cryptologically sophisticated countries and, from them, gained insight into plans and intentions of countries about which the US has greater concerns. Thus, when a Chinese diplomat at the United Nations discusses some new African venture with a colleague from Sudan, the eavesdroppers at the NSA may be deaf to the Chinese communications links but they may be able to get that same information by exploiting weaknesses in Sudan's communications and cipher systems when the diplomat reports the meeting to Khartoum. But even third-world cryptography can be daunting. During the entire war in Vietnam, writes Aid, the agency was never able to break the high-level encryption systems of either the North Vietnamese or the Vietcong. It is a revelation that leads him to conclude "that everything we thought we knew about the role of NSA in the Vietnam War needs to be reconsidered."

Because the book is structured chronologically, it is somewhat difficult to decipher the agency's overall record. But one sees troubling trends. One weakness that seems to recur is that the agency, set up in the wake of World War II to prevent another surprise attack, is itself frequently surprised by attacks and other serious threats. In the 1950s, as over 100,000 heavily armed North Korean troops surged across the 38th parallel into South Korea, the codebreakers were among the last to know. "The North Korean target was ignored," says a declassified NSA report quoted by Aid. "North Korea got lost in the shuffle and nobody told us that they were interested in what was going on north of the 38th parallel," exclaimed one intelligence officer. At the time, astonishingly, the Armed Forces Security Agency (AFSA), the NSA's predecessor, didn't even have a Korean-language dictionary.

Unfortunately for General Douglas MacArthur, the codebreakers were able to read the communications of Spain's ambassador to Tokyo and

other diplomats, who noted that in their discussions with the general, he made clear his secret hope for all-out war with China and Russia, including the use of nuclear weapons if necessary. In a rare instance of secret NSA intercepts playing a major part in US politics, once the messages were shown to President Truman, MacArthur's career abruptly ended.

Another major surprise came in the 1960s when the Soviet Union was able to move large numbers of personnel, large amounts of equipment, and many ballistic missiles to Cuba without the NSA hearing a peep. Still unable to break into the high-level Soviet cipher systems, the agency was unaware that the 51st Rocket Division had packed up and was encamped in Cuba. Nor did it detect the move of five complete medium-range and intermediate-range missile regiments from their Russian bases to Cuba. And it had no knowledge that Russian ballistic missiles were on Cuban soil, being positioned in launchers. "Soviet communications security was almost perfect," according to an NSA historian.

The first clues that something unusual was happening had come in mid-July 1962, when NSA analysts noticed record numbers of Soviet cargo and passenger ships heading for Cuba. Analysis of their unencrypted shipping manifests led the NSA to suspect that the ships were delivering weapons. But the nuclear-armed ballistic missiles were not detected until mid-October, a month after their arrival, and not by the NSA; it was the CIA, acting on information from its sources in Cuba and Florida, that ordered the U-2 reconnaissance flight that photographed them at launch sites on the island. "The crisis," Aid concludes, "was in fact anything but an intelligence success story." This is a view shared by the agency itself in a candid internal history, which noted that the harrowing events "marked the most significant failure of SIGINT [signals intelligence] to warn national leaders since World War II."

More recently, the NSA was unaware of India's impending nuclear test in 1998, the 1993 attack on the World Trade Center, the attack on the USS *Cole* in 2000, and the 1998 bombing of two of America's East African embassies. The agency first learned of the September 11 attacks on $300 television sets tuned to CNN, not its billion-dollar eavesdropping satellites tuned to al-Qaeda.

Then there is the pattern by which the NSA was actually right about a warning, but those in power chose to ignore it. During the Korean War, the AFSA picked up numerous indications from low-level unencrypted Chinese intercepts that the Chinese were shifting hundreds of thousands of combat troops to Manchuria by rail, an obvious signal that China might enter the war. But those in charge of Army intelligence simply refused to believe it; it didn't fit in with their plans.

Then, by reading the dispatches between India's well-connected ambassador to Beijing and his Foreign Office, it became clear that China would intervene if UN forces crossed the 38th parallel into North Korea. But again, says Aid, the warning "was either discounted or ignored completely by policymakers in Washington," and as the UN troops began crossing the divide, Chinese troops crossed the Yalu River into North Korea. Even when intercepts indicated that the Chinese were well entrenched in the North, officials in Washington and Seoul remained in a state of disbelief, until both South Korean and US forces there were attacked by the Chinese forces.

The pattern was repeated in Vietnam when NSA reporting warned on January 25, 1968, that a major coordinated attack would occur "in the near future in several areas of South Vietnam." But neither the White House, the CIA, nor General William Westmoreland at US military headquarters in Saigon believed it, until over 100,000 North Vietnamese and Vietcong troops launched their Tet offensive in the South five days later on January 30. "The [NSA] reports failed to shake the commands in Washington and Saigon from their perception," says an NSA history. Tragically, Aid notes, at the end of the war, all of the heroic Vietnamese cryptologic personnel who greatly helped the NSA were left behind. "Many," the NSA report reveals, "undoubtedly perished." It added, "Their story is yet untold." Then again in 1973, as in Korea and Vietnam, the NSA warned that Egypt and Syria were planning "a major offensive" against Israel. But, as Aid quotes an official NSA history, the CIA refused to believe that an attack was imminent "because [they thought] the Arabs wouldn't be 'stupid enough' to attack Israel." They were, they did, and they won.

Everything seemed to go right for the NSA during the Soviet invasion of Afghanistan, which the agency had accurately forecast. "NSA predicted on December 22 [1979], three full days before the first Soviet troops crossed the Soviet–Afghan border, that the Russians would invade Afghanistan within the next seventy-two hours," writes Aid, adding, "Afghanistan may have been the 'high water mark' for NSA."

The agency also recorded the words of the Russian fighter pilot and his ground controllers as he shot down Korean Airlines Flight 007 in 1983. Although the agency knew that the Russians had accidently mistaken the plane for a potentially hostile US military aircraft, the Reagan administration nevertheless deliberately spun the intercepts to make it seem that the fighter pilot knew all along that it was a passenger jet, infuriating NSA officials. "The White House's selective release of the most salacious of the NSA material concerning the shootdown set off a firestorm of criticism inside NSA," writes Aid. It was not the first time, nor would it be the last, that the NSA's product was used for political purposes.

The most troubling pattern, however, is that the NSA, through gross incompetence, bad intelligence, or deliberate deception through the selective release of information, has helped to push the US into tragic wars. A prime example took place in 1964 when the Johnson administration claimed that two US Navy destroyers in the Gulf of Tonkin, one on an eavesdropping mission for the NSA, were twice attacked by North Vietnamese torpedo boats. Those attacks were then used to justify the escalation of American involvement in the Vietnam War. But Aid cites a top-secret NSA analysis of the incident, completed in 2000, which concluded that the second attack, the one used to justify the war, never took place. Instead, NSA officials deliberately withheld 90 percent of the intelligence on the attacks and told the White House only what it wanted to hear. According to the analysis, only intelligence "that supported the claim that the communists had attacked the two destroyers was given to administration officials."

Not having learned its lesson, in the lead-up to the war in Iraq the NSA again told the administration only what it wanted to hear, despite the clearly ambiguous nature of the evidence. For years beforehand, the agency's coverage of Iraq was disastrous. In the late 1990s, the Iraqis began shifting much of their high-level military communications from radio to buried fiber optic networks, and at the same time, Saddam Hussein banned the use of cell phones. That left only occasional low-level troop communications. According to a later review, Aid writes, NSA had "virtually no useful signals intelligence on a target that was one of the United States' top intelligence priorities." And the little intelligence it did have pointed away from Iraq possessing weapons of mass destruction. "We looked long and hard for any signs," said one retired NSA official. "We just never found a 'smoking gun' that Saddam was trying to build nukes or anything else." That, however, did not prevent the NSA director, Lieutenant Gen. Michael V. Hayden, from stamping his approval on the CIA's 2002 National Intelligence Estimate arguing that Iraq's WMDs posed a grave danger, which helped prepare the way for the devastating war.

While much of the terrain Aid covers has been explored before, the most original areas in *The Secret Sentry* deal with the ground wars in Afghanistan and Iraq, where the NSA was forced to marry, largely unsuccessfully, its super-high-tech strategic capabilities in space with its tactical forces on the ground. Before the September 11 attacks, the agency's coverage of Afghanistan was even worse than that of Iraq. At the start of the war, the NSA's principal listening post for the region did not have a single linguist proficient in Pashto or Dari, Afghanistan's two principal languages. Agency recruiters descended on Fremont, California, home of the country's largest population of Afghan expatriates, to build up a cadre of translators—only to have most candidates rejected by the agency's overparanoid security experts. On the plus side, because of the collapse of the Taliban regime's rudimentary communications system, its leaders were forced to communicate only by satellite phones, which were very susceptible to NSA monitoring.

Other NSA tactical teams, Aid explains, collaborated on the ground with Special Forces units, including in the mountains of Tora Bora. But it was a new type of war, one the NSA was not prepared for, and both Osama bin Laden and Taliban leader Mullah Omar easily slipped through its electronic net. Eight years later, despite billions of dollars spent by the agency and dozens of tapes released by bin Laden, the NSA is no closer to capturing him or Mullah Omar than it was at Tora Bora in 2001.

Disappointingly, the weakest section of the book, mostly summaries of old news clips, deals with what may be the most important subject: the NSA's warrantless eavesdropping and its targeting of American communications. There is no discussion, for example, of the agency's huge data-mining centers, mentioned above, currently being built in Utah and Texas, or to what extent the agency, which has long been confined to foreign and international communications, is now engaged in domestic eavesdropping.

It is a key question and we have no precise answer. By installing its intercept rooms in such locations as AT&T's main switching station in downtown San Francisco, the agency has physical access to domestic as well as international communications. Thus it is possible that the agency scans all the e-mail of both and it may also eavesdrop on the telephone calls of both for targets on its ever-growing watch lists. According to a recent Justice Department report, "As of December 31, 2008, the consolidated terrorist watchlist contained more than 1.1 million known or suspected terrorist identities."[3]

Aid's history becomes thin as it gets closer to the present day and the archival documents dwindle, especially since he has no substantial first-person, on-the-record interviews. Beyond a brief mention, he also leaves other important aspects of the NSA's history unaddressed, including the tumultuous years in the mid-1970s when it was investigated by the Senate's Church Committee for decades of illegal spying; Trailblazer, the nearly decade-long failure to modernize the agency; and the NSA's increasingly important role in cyberwarfare and its implications in future wars.

Where does all this leave us? Aid concludes that the biggest problem facing the agency is not the fact that it's drowning in untranslated, indecipherable, and mostly unusable data, problems that the troubled new modernization plan, Turbulence, is supposed to eventually fix. "These problems may, in fact, be the tip of the iceberg," he writes. Instead, what the agency needs most, Aid says, is more power. But the type of power to which he is referring is the kind that comes from electrical substations, not statutes. "As strange as it may sound," he writes, "one of the most urgent problems facing NSA is a severe shortage of electrical power." With supercomputers measured by the acre and estimated $70 million annual electricity bills for its headquarters, the agency has begun browning out, which is the reason for locating its new data centers in Utah and Texas. And as it pleads for more money to construct newer and bigger power generators, Aid notes, Congress is balking.

The issue is critical because at the NSA, electrical power *is* political power. In its top-secret world, the coin of the realm is the kilowatt. More electrical power ensures bigger data centers. Bigger data centers, in turn, generate a need for more access to phone calls and e-mail and, conversely, less privacy. The more data that comes in, the more reports flow out. And the more reports that flow out, the more political power for the agency.

Rather than give the NSA more money for more power—electrical and political—some have instead suggested just pulling the plug. "NSA can point to things they have obtained that have been useful," Aid quotes former senior State Department official Herbert Levin, a longtime customer of the agency, "but whether they're worth the billions that are spent, is a genuine question in my mind."

Based on the NSA's history of often being on the wrong end of a surprise and a tendency to mistakenly get the country into, rather than out of, wars, it seems to have a rather disastrous cost-benefit ratio. Were it a corporation, it would likely have gone belly-up years ago. The September 11 attacks are a case in point. For more than a year and a half the NSA was eavesdropping on two of the lead hijackers, knowing they had been sent by bin Laden, while they were in the US preparing for the attacks. The terrorists even chose as their command center a

motel in Laurel, Maryland, almost within eyesight of the director's office. Yet the agency never once sought an easy-to-obtain FISA warrant to pinpoint their locations, or even informed the CIA or FBI of their presence.

But pulling the plug, or even allowing the lights to dim, seems unlikely given President Obama's hawkish policies in Afghanistan. However, if the war there turns out to be the train wreck many predict, then Obama may decide to take a much closer look at the spy world's most lavish spender. It is a prospect that has some in the Library of Babel very nervous. "It was a great ride while it lasted," said one.

### Notes

[1]The MITRE Corporation, "Data Analysis Challenges" (December 2008), p. 13.

[2]David Leppard, "Internet Firms Resist Ministers' Plan to Spy on Every E-mail,"*The Sunday Times* , August 2, 2009.

[3]"The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices," US Department of Justice, Office of the Inspector General, Audit Division, Audit Report 09-25, May 2009.

http://www.nybooks.com/articles/23231