Written by **Charles Scaliger** on May 10, 2012

The Surveillance State: Knowing Every Bit About You

No one ever accused Jeremy Bentham of thinking small. The early 18th-century British philosopher, social reformer, and co-founder of the celebrated philosophical school of Utilitarianism, Bentham was known for his unconventional ideas. Like many self-styled progressive thinkers of his age, Bentham expended a considerable amount of energy dreaming up new ways to use the power of the state to protect private citizens from their own alleged follies.

The concept of the Panopticon was probably Bentham's best-known brainchild. An extravagant idea for its time, it has proven an enduring metaphor in our time and — far more importantly — prefigured our modern obsession with high-tech surveillance. Derived from Greek roots that mean "all-seeing," Bentham's Panopticon was a building designed to house many people in close quarters whose rooms were so configured that a central authority, using a system of tubes and mirrors, could keep every inmate under constant surveillance. The Panopticon concept could be applied to prisons, factories, or any place where large numbers of people would live or work in close quarters. "Morals reformed — health preserved — industry invigorated — instruction diffused — public burthens [burdens] lightened — economy seated, as it were, upon a rock — the Gordian knot of the poor-law not cut, but untied — all by a simple idea in architecture," Bentham enthused, proclaiming that his Panopticon represented "a new mode of obtaining power of mind over mind, in a quantity hitherto without example." The energetic Bentham tried to persuade the British government to let him design a Panopticon prison, but was ultimately unsuccessful. Although he managed to persuade Prime Minister William Pitt the Younger of the Panopticon's potential, Pitt's successor shut down the project.

But Bentham's premise — of a system of comprehensive state surveillance to guarantee a pliant and docile citizenry — is still with us, magnified by the potency of 21st-century technology and zealously promoted the world over, but especially in Western nations, like Great Britain and the United States, that once viewed such state activities as abhorrent and dangerous to liberty. A decade after the defining crisis of our era, the terrorist attacks of 9/11, the United States of America is on the verge of becoming a Panopticon society, with powers of state surveillance far beyond the most fevered imaginings of Bentham and fellow pre-modern utopians.

Panopticon Society

In the sagebrush desert of Bluffdale, Utah, in the shadow of the Wasatch Mountains, a vast new federal surveillance and intelligence processing center is being erected. The so-called Utah Data Center, operated by the National Security Agency, will occupy more than a million square feet when it becomes operational sometime next year. Within its ultra-secure perimeter, surveillance on a scale never before achieved will be carried out, of a vast array of digital communications — cellphone conversations, e-mails, Google searches, and the like — both on foreign and domestic soil. Thanks to significant (and highly classified) advances in decryption technology, coupled with unprecedented supercomputing power, the new facility will be the nerve center for near-total surveillance capabilities over hundreds of

millions of Americans. If the Utah Data Center fulfills it ominous potential, the cherished American right to privacy will have no more substance.

But the Bluffdale facility is merely the culmination of an aggressive new effort to bring all of Americans' private activities under at least potential surveillance by the feds, an effort undertaken soon after the 9/11 attacks. The first attempt to create what *New York Times* columnist William Safire called "computer dossiers on 300 million Americans" was launched in 2002. Under the leadership of John Poindexter, former National Security Advisor under Ronald Reagan, the Information Awareness Office (IAO) was created within the Defense Advanced Research Projects Agency (DARPA). Its goal, well-publicized at the time, was "total information awareness," the warrantless compilation of vast databases on the private financial activities and communications of every single American — their credit card activity, e-mails, social networks, phone calls, airline ticket purchases, car rentals, and so forth. This data would then be analyzed to look for suspicious patterns of behavior, evidence of potential terrorist activity.

From the outset, DARPA and the IAO generated a lot of bad publicity, driven in no small measure by the former's genuinely spooky choice of logo: the all-seeing eye atop a pyramid (also depicted on the back of the dollar bill) gazing godlike at the entire world, accompanied by the motto "Cientia est Potentia" ("Knowledge is Power"). By 2003, the public and congressional hue and cry over what was transparently an extra-constitutional program had become so great that Congress officially defunded the IAO.

But like the stereotyped villain in a slasher film that cannot be killed, much of the work carried out by the IAO was merely transferred to other branches of America's vast security establishment. While Congress tried to stipulate that none of the new tools being developed could be used against American citizens or on American soil, the drive to develop more powerful supercomputers with the ability to compile more and more comprehensive data profiles of anybody, anywhere, continued throughout the last decade. And it is by no means clear whether the federal government did, in fact, refrain from spying on its own citizens during that period; if the testimony of certain disgruntled former NSA employees is to believed, quite the opposite is true. According to William Binney, a former senior cryptographer and mathematician at the NSA, the storied and notoriously closemouthed security agency has systematically flouted and circumvented all congressional limits on intelligence gathering ever since 9/11, ignoring in some cases restrictions on spying on Americans that date from the post-Watergate era. Speaking of the launching of "warrantless wiretapping" soon after 9/11, Binney, who resigned in disgust after four decades of code breaking, did not mince words. "They violated the Constitution setting it up," he told *Wired* magazine's James Bamford. "But they didn't care. They were going to do it anyway, and they were going to crucify anyone who stood in the way. When they started violating the Constitution, I couldn't stay."

Toys for Tracking Us

According to Binney, the program, codenamed Stellar Wind, intercepted without warrant not only domestic phone calls but domestic e-mails as well. At the very beginning, the NSA was intercepting 320 million domestic phone calls per day — and the number quickly expanded. Bamford relates:

> According to Binney — who has maintained close contact with agency employees until a few years ago — the taps in the secret rooms dotting the country are actually powered by highly sophisticated software programs that conduct "deep packet inspection," examining Internet traffic as it passes through the 10-gigabit-per-second cables at the speed of light.

The software, created by a company called Narus that is now part of Boeing, is controlled remotely from NSA headquarters at Fort Meade in Maryland and searches US sources for target addresses, locations, countries, and phone numbers, as well as watch-listed names, keywords, and phrases in email. Any communication that arouses suspicion, especially those to or from the million or so people on agency watch lists, are automatically copied or recorded and then transmitted to the NSA.

The scope of surveillance expands from there, Binney says. Once a name is entered into the Narus database, all phone calls and other communications to and from that person are automatically routed to the NSA's recorders. "Anybody you want, route to a recorder," Binney says. "If your number's in there? Routed and gets recorded." He adds, "The Narus device allows you to take it all." And when the Bluffdale facility is completed, whatever is collected will be routed there for storage and analysis.

According to Binney, one of the deepest secrets of the Stellar Wind program — again, never confirmed until now — was that the NSA gained warrantless access to AT&T's vast trove of domestic and international billing records, detailed information about who called whom in the US and around the world. As of 2007, AT&T had more than 2.8 trillion records housed in a database at its Florham Park, New Jersey, complex.

Verizon was also part of the program, Binney says, and that greatly expanded the volume of calls subject to the agency's domestic eavesdropping. "That multiplies the call rate by at least a factor of five," he says. "So you're over a billion and a half calls a day." (Spokespeople for Verizon and AT&T said their companies would not comment on matters of national security.)

The NSA also has the ability to eavesdrop on telephone conversations in real time, whenever it deems appropriate. In the months and years following 9/11, any excuse would do, especially for family members abroad calling home to the United States. Adrienne J. Kinne, who worked as a voice interceptor for the NSA both before and after the 9/11 attacks, told *Wired*, "Basically all rules were thrown out the window, and they would use any excuse to justify a waiver to spy on Americans." Journalists working overseas were routinely eavesdropped upon whenever they called their families stateside. "A lot of time you could tell they were calling their families," Kinne admitted, "incredibly intimate, personal conversations." Kinne likened the practice to finding someone's personal diary and going through it.

But the NSA's suffocating blanket of surveillance has one major hole — the ability of modern encryption protocols like the Advanced Encryption Standard (AES) to resist decryption, even by the most powerful supercomputers available. The solution? Build still more powerful supercomputers, machines capable of carrying out one quadrillion (1015) operations per second, a capability known in industry jargon as a "petaflop." Accordingly, what has been characterized as nothing less than a modern-day Manhattan Project, the High Productivity Computing Systems program, was begun in 2004 to develop computers with just such a capacity. That the research and development for the project was and is being carried out at the Oak Ridge National Laboratory in Tennessee — the same place where uranium was enriched for the first atomic bombs — is perhaps an unintended irony. But this time around, America's best and brightest are devising a superweapon not for deployment against a distant foreign military power, but against our own citizens, to finally ensure that any degree of privacy whatsoever can be breached by Washington's all-seeing eye.

By all accounts, the High Productivity Computing Systems program has been a stunning success. An unclassified program at Oak Ridge produced the so-called "Jaguar," an upgraded Cray XT5 supercomputer that clocked in as the world's fastest in 2009 — at a rate of 1.75 petaflops. A top-secret

program, also at Oak Ridge, has reputedly created machines faster still, whose exact capabilities remain a closely guarded secret.

And the NSA is already setting its sights on new orders of computing power magnitude — the exaflop (one quintillion, or 1018 operations a second) being its goal for 2018, and other, more exotic levels beyond that (the zettaflop/1021 operations per second and the yottaflop/1024). When such mind-boggling computing power becomes available, as it eventually must (consider that the world's official fastest computer as of this writing is a Japanese supercomputer operating at more than 10 petaflops), current encryption protocols like the AES will become obsolete. If the NSA manages to develop such a capability in secret, as it clearly aims to do, private-sector encryption will be none the wiser, leaving essentially all encrypted communications as bare to government code-breakers as the Germans' best codes in World War II eventually were to the Allies.

For it is nothing less than a terminal war on Americans' privacy that is being waged, in deep secrecy and by a comparatively small and fanatically dedicated group of government security fetishists. And the supercomputers that are to dismantle the final barricades protecting communications privacy will be no less a power trump card in the hands of the state than nuclear weapons have proven to be for the world's elite military powers.

Overlooking From Overhead

The government's new powers of surveillance will not be limited to supercomputers tracking our every act of private electronic computation. The advent of unmanned drones, a legacy of the war in Afghanistan, will soon transform law enforcement at every level. For the cost of one police helicopter that can only be in one place at a time, a given jurisdiction could deploy dozens of remotely piloted drones to overfly restive neighborhoods and keep tabs on backyards and open windows as well as public areas.

This is not idle speculation. In February, Congress passed the FAA Reauthorization Act, which is transparently calculated to streamline the introduction of unmanned drones, for federal, state, and local law enforcement and surveillance, into U.S. domestic airspace. U.S. Customs and Border Protection already operate nine Predator-type drones, chiefly for border surveillance, under four long-term FAA certificates. But the new legislation in effect orders the FAA to develop an expedited protocol, by year's end, for authorizing the use of unmanned drones by law enforcement at every level, as well as any other government agency (read: Homeland Security, one agency that has made no secret of its desire to operate a fleet of drones in domestic airspace) that wants to use them.

The legislation has appalled privacy advocates. By one estimate, once the FAA floodgates are opened, American skies may be populated with as many as 30,000 drones by the end of this decade, all busily keeping tabs on any activity not carried out in basements or behind closed doors and covered windows.

Then there is the ongoing drive to desensitize Americans to having to stand naked before the state, as is now required for those who wish to board an airplane within the United States. Backscatter imaging machines, which digitally strip-search passengers as they pass through security, have proliferated rapidly and will soon be found in every commercial airport in the land, if the TSA has any say in the matter. These machines produce finely detailed images of naked bodies, images with high enough resolution to display colostomy bags, breast prostheses, and every intimate detail of the human body. Those who object may opt out of being digitally strip-searched — and must instead submit to intrusive pat-downs in which TSA agents will touch the most intimate parts of the body.

Not Nice Nakedness

These machines are now being introduced in train stations and courthouses as well, as naked becomes the new normal. A recent Supreme Court decision upholding the "right" of police to strip-search anyone arrested for any reason (the plaintiff, Albert Florence, was strip-searched twice after being arrested for an unpaid traffic fine) gives legal countenance to the dangerous notion that state-sanctioned strip-searches of anyone, anywhere, anytime are perfectly acceptable in the post 9/11 world.

But as Naomi Wolf of the *Guardian* has recently pointed out, allowing the state to strip us (literally) of one of the last vestiges of privacy — our clothing — is both symbolically and practically one of the most potent symptoms of a police state:

> Believe me: you don't want the state having the power to strip your clothes off. History shows that the use of forced nudity by a state that is descending into fascism is powerfully effective in controlling and subduing populations.

The political use of forced nudity by anti-democratic regimes is long established. Forcing people to undress is the first step in breaking down their sense of individuality and dignity and reinforcing their powerlessness. Enslaved women were sold naked on the blocks in the American south, and adolescent male slaves served young white ladies at table in the south, while they themselves were naked: their invisible humiliation was a trope for their emasculation. Jewish prisoners herded into concentration camps were stripped of clothing and photographed naked, as iconic images of that Holocaust reiterated.

One of the most terrifying moments for me when I visited Guantanamo prison in 2009 was seeing the way the architecture of the building positioned glass-fronted shower cubicles facing intentionally right into the central atrium — where young female guards stood watch over the forced nakedness of Muslim prisoners, who had no way to conceal themselves. Laws and rulings such as [the recent Supreme Court ruling upholding strip searches of anyone arrested] are clearly designed to bring the conditions of Guantanamo, and abusive detention, home.

The spanking-new total surveillance state requires legal camouflage, given that so much of its newfound powers of surveillance (in effect, the "search" part of "search and seizure" with which the authors of the Bill of Rights were so concerned) is carried out without the warrants and probable cause required by the Fourth Amendment. Adherence to the letter of this amendment — which stipulates that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" — would appear to preclude warrantless surveillance by drones and supercomputer algorithms, as well as digital and literal strip-searches without probable cause by airport authorities and law enforcement generally.

Where Is the Constitution?

But the Fourth Amendment has proven no impediment to the homeland security fetishists, from the President on down, thanks to a Congress congenitally unwilling to challenge the relentless advance of Big Security. It was Congress, after all, that produced the National Defense Authorization Act for Fiscal Year 2012 (NDAA), which President Obama coyly signed on the last day of 2011, when the nation was preoccupied with holiday celebrations. This act gave legal cover to the actions of the U.S. government since 9/11 in detaining indefinitely and without trial persons alleged to have committed hostile acts against the United States. The NDAA not only explicitly authorizes such detentions (in section 1021) but also (section 1022) requires that detainees under this provision be held in military custody, either within the United States or on foreign soil.

Meanwhile, the Supreme Court, in what must surely be regarded as one of its most pernicious rulings since *Roe v. Wade*, has inexplicably upheld the right of law-enforcement authorities, whether local, state, or national, to strip-search anyone arrested for any reason, in *Florence v. Board of Chosen Freeholders of County of Burlington*. The specious grounds for this ruling are the possibility that someone arrested could have a weapon or contraband concealed somewhere on or inside his body, thereby posing a threat to authorities and other inmates. "Correctional officials have a significant interest in conducting a thorough search as a standard part of the intake process," wrote Justice Anthony Kennedy on behalf of the majority that included all of the Supreme Court's supposed "right-wing" and "conservative" justices.

For once, the "liberal" minority got it right. "I cannot find justification for the strip-search policy at issue here — a policy that would subject those arrested for minor offenses to serious invasions of their personal privacy," wrote Justice Ruth Bader Ginsburg. She might well have added that people — even criminals — generally do not walk around with weapons and narcotics concealed inside their bodies, in anticipation of possible arrest and imprisonment. It is patently absurd to justify strip searches of traffic violators as though they were hardened criminals trying to smuggle contraband to others "on the inside." Yet that is precisely the kind of non-logic that undergirds the Supreme Court's latest usurpation.

The total loss of privacy coupled with aggressively expanding powers of the state to encroach on our personal freedoms with impunity — these are the two prongs of the police-state pincers that are closing swiftly on American liberties. The long-feared "garrison state" is coming into being on American soil before our very eyes, with the approval, tacit or overt, of millions of Americans who believe that the only way to guarantee national security is to deprive us of personal security (the Fourth Amendment, after all, protects the "right of the people to be *secure*" against government encroachment on a personal level). In a coming day, unless the tide of Big Government is stemmed, we will all find ourselves living in a hi-tech Panopticon stretching from sea to shining sea.

Somewhere, Bentham's shade is smiling.