GlobalResearch
Center for Research on Globalization

Institutionalized Spying on Americans

Homeland Security's National Applications Office (NAO)

By Stephen Lendman
Global Research, January 17, 2008
17 January 2008

Region: USA
Theme: Police State & Civil Rights

This article reviews two police state tools (among many in use) in America. One is new, undiscussed and largely unknown to the public. The other was covered in a December article by this writer called Police State America. Here it is updated with new information.

The National Applications Office (NAO)

The Department of Homeland Security (DHS) established a new domestic spying operation in 2007 called the National Applications Office (NOA) and described it as "the executive agent to facilitate the use of intelligence community technological assets for civil, homeland security and law enforcement purposes within the United States." The office was to begin operating last fall to "build on the long-standing work of the Civil Applications Committee (CAC), which was created in 1974 to facilitate the use of the capabilities of the intelligence community for civil, non-defense uses in the United States."

With or without congressional authorization or oversight, the executive branch is in charge and will let NAO use state-of-the-art technology, including military satellite imagery, to spy on Americans without their knowledge. Implementation is delayed, however, after Committee on Homeland Security Chairman, Bennie Thompson, and other committee members raised questions of "very serious privacy and civil liberties concerns." In response, DHS agreed to delay operating (officially) until all matters are addressed and resolved.

Given its track record post-9/11, expect little more than pro forma posturing before Congress signs off on what Kate Martin, the director of the Center for National Security Studies, calls "Big Brother in the Sky" and a "police state" in the offing.

DHS supplies this background information on NAO. Post-9/11, the Director of National Intelligence appointed an Independent Study Group (ISG) in May, 2005 to "review the current operation and future role of the (1974) Civil Applications Committee and study the current state of Intelligence Community support to homeland security and law enforcement entities."

In September 2005, the Committee produced a "Blue Ribbon Study," now declassified. Its nine members were headed by and included three Booz Allen Hamilton officials because of the company's expertise in spying and intelligence gathering. Its other members have similar experience. They all have a vested interest in domestic spying because the business potential is huge for defense related industries and consultants.

ISG members included:

Keith Hall, Chairman
Vice President, Booz Allen Hamilton

Edward G. Anderson
LTG US Army (Ret),
Principal, Booz Allen Hamilton

Thomas W. Conroy
Vice President
National Security Programs
Northrop Grumman/TASC

Patrick M. Hughes
LTG US Army (Ret)
Vice President, Homeland Security
L-3 Communications

Kevin O'Connell
Director of Defense Group Incorporated (DGI)
Center for Intelligence Research and Analysis (CIRA)

CIRA is a think tank that calls itself "the premier open source and cultural intelligence exploitation cell for the US intelligence community." Its business is revolutionizing intelligence analysis.

Jeff Baxter
Independent Defense Consultant with DOD and industry ties

Dr. Paul Gilman
Director
Oak Ridge Center for Advanced Studies

Oak Ridge National Laboratory
US Department of Energy

Kemp Lear
Associate
Booz Allen Hamilton, and

Joseph D. Whitley, Esq
Alston & Bird LLP, Government Investigations and Compliance Group, former Acting Associate Attorney General in GHW Bush administration, and former General Counsel for DHS under GW Bush

The ISG's report produced 11 significant findings and 27 recommendations based on its conclusion that there's "an urgent need for action because opportunities to better protect the nation are being missed." It "concluded a new management and process model (is) needed to effectively employ IC (Intelligence Community) capabilities for domestic uses."

In March 2006, DHS unveiled the new agency to implement ISG's recommendations called the National Applications Office. In May, 2007, Director of National Intelligence (DNI), Michael McConnell, named DHS as its executive agent and functional manager. At least in

principle according to DHS, Congress agreed with this approach and to provide funding for it, beginning in the fall of 2007.

The public knew nothing about this until a feature August 15, 2007 Wall Street Journal story broke the news. It was headlined “US to Expand Use of Spy Satellites.” It noted that for the first time the nation’s top intelligence official (DNI’s McConnell) “greatly expanded the range of federal and local (civilian law enforcement agencies that) can get access to” military spy satellite collected information. Until now, civilian use was restricted to agencies like NASA and the US Geological Survey, and only for scientific and environmental study.

The Journal explained that key objectives under new guidelines will be:

> — border security,
>
> — securing critical infrastructure and helping emergency responders after natural disasters,
>
> — working with criminal and civil federal, state, and local law enforcement agencies, and
>
> — unmentioned by the Journal, the ability to spy on anyone, anywhere, anytime domestically for any reason – an unprecedented act using state-of-the-art technology enabling real-time, high-resolution images and data from space.

NAO will also oversee classified information from the National Security Agency (NSA), the National Geospatial-Intelligence Agency (NGA) and other US agencies involved in dealing with all aspects of national security, including “terrorism.”

NSA was established in 1952, is super-secret, and for many years was never revealed to exist. Today, its capabilities are awesome and worrisome. It eavesdrops globally, mines a vast amount of data, and does it through a network of spy satellites, listening posts, and surveillance planes to monitor virtually all electronic communications from landline and cell phones, telegrams, emails, faxes, radio and television, data bases of all kinds and the internet.

NGA is new and began operating in 2003. It lets military and intelligence analysts monitor virtually anything or anyone from state-of-the-art spy satellites. Both NSA and NGA coordinate jointly with the National Reconnaissance Office (NRO) that designs, builds and operates military spy satellites. It also analyzes military and CIA-collected aircraft and satellite reconnaissance information.

Combined with warrantless wiretapping, pervasive spying of all kinds, the abandonment of the law and checks and balances, intense secrecy, and an array of repressive post-9/11 legislation, Executive Orders and National Security and Homeland Security Presidential Directives, NAO is another national security police state tool any despot would love. It’s now established and may be operating without congressional approval.

Using spy satellites domestically “is largely uncharted territory,” as the Wall Street Journal noted. Even its architects admit there’s no clarity on this, and the ISG’s report stated “There is little if any policy, guidance or procedures regarding the collection, exploitation and dissemination of domestic MASINT (Measurement and Signatures Intelligence).”

The Defense Intelligence Agency (DIA) is the main DOD spy agency. It manages MASINT that's ultra-secret and sophisticated. It uses state-of-the-art radar, lasers, infrared sensors, electromagnetic data and other technologies that can detect chemicals, electro-magnetic activity, whether a nuclear power plant produces plutonium, and the type vehicle from its exhaust. It can also see under bridges, through clouds, forest canopies and even concrete to create images and collect data. In addition, it can detect people, activity and weapons that satellites and photo-reconnaissance aircraft miss, so it's an invaluable spy tool but highly intrusive and up to now only for military and foreign intelligence work.

Further, military spy satellites are state-of-the-art and superior to civilian ones. They record in color as well as black and white, use different parts of the light spectrum to track human activities and ground movements and can detect chemical weapons traces and people-generated heat in buildings.

This much we know about them. Their full potential is top secret and available only to the military and intelligence community. The Journal quoted an alarmed Gregory Nojeim, senior counsel and director of the Project on Freedom, Security and Technology, that advocates for digital age privacy rights saying: "Not only is the surveillance they are contemplating intrusive and omnipresent, it's also invisible. And that's what makes this so dangerous."

Anyone for any reason may be watched at all times (through walls) with no way to know it, but a June 2001 (before 9/11) Supreme Court decision offers hope. In Kyllo v. United States, the Court ruled for petitioner 5 to 4 (with Scalia and Thomas in the majority). It voided a conviction based on police use of thermal imaging to detect heat in his triplex to determine if an illegal drug was being grown, in this case marijuana.

The Court held: "Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search," and is presumptively unreasonable without a warrant….To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment" protecting against "unreasonable searches and seizures."

In 1981, Ronald Reagan seemed to agree in Executive Order 12333 on United States Intelligence Activities. It bars the intelligence community from most forms of home eavesdropping while providing wide latitude to all government agencies to "provide the President and the National Security Council with the necessary information (needed to) conduct….foreign, defense and economic policy (and protect US) national interests from foreign security threats. (Collecting this information is to be done, however,) consistent with the Constitution and applicable law…."

That was then, and this is now. It's hard imagining congressional concern or DHS meaning that NAO will "prioritize the protection of privacy and civil liberties" and citing the Reagan Executive Order and the 1974 Privacy Act. That law mandates that no government agency "shall disclose any record (or) system of records by any means of communication to any person, or to another agency, except pursuant to a written request, or with the prior written consent of, the individual to whom the record pertains." The Privacy act requires the US government to maintain an administrative and physical security system to prevent the unauthorized release of personal records.

Post-9/11, the Patriot Act ended that protection, so DHS is shameless saying NAO must comply with civil liberties and privacy laws and be subject to "oversight by the DHS Inspector General, Chief Privacy Officer, and the Officer for Civil Rights and Liberties" plus additional oversight. No longer post-9/11 when the national security state got repressive new tools to erode the constitution, ignore democratic principles, and give the President unrestricted powers in the name of national security. NAO is the latest one watching us as our "Big Brother in the Sky." Orwell would be proud.

Real ID Act Update – Another Intrusive Police State Tool

The Read ID Act of 2005 required states to meet federal ID standards by May, 2008. That's now changed because 29 states passed or introduced laws that refuse to comply. They call the Act costly to administer, a bureaucratic nightmare, and New Hampshire said it's "repugnant" and violates the state and US Constitutions.

The federal law mandates that every US citizen and legal resident have a national ID card that in most cases is a driver's license meeting federal standards. It requires it to contain an individual's personal information and makes one mandatory to open a bank account, board an airplane, be able to vote, get a job, enter a federal building, or conduct virtually all essential business requiring identification.

States balked, and that doomed the original version. On January 11, changes were unveiled when the Department of Homeland Security (DHS) issued binding new rules. Under them, states have until 2011 to comply (instead of 2008), until 2014 to issue "tamper-proof licenses" to drivers born after 1964, and until 2017 for those born before this date. DHS said the original law would cost states $14 billion. The new regulations with an extended phase-in cuts the amount to around $3.9 billion or $8 per license.

These numbers may be bogus, however, the true costs may be far higher, and that's why the Information Technology Association of America (ITAA) is lobbying for Real ID's passage. Its members include high-tech card makers like Digimarc and Northrup Grumman and data brokers like Choicepoint and LexisNexis that profit by selling personal information to advertisers and the government.

Under new DHS rules, licenses must include a digital photo taken at the beginning of the application process and a filament or other security device to prevent counterfeiting. They must also have three layers of security that states can select from a DHS menu. In addition, states must begin checking license applicants' Social Security and immigration status over the next year.

As of now, a controversial radio frequency identification (RFID) technology microchip isn't required. It may come later, however, and here's the problem. It'll let cardholder movements and activities be tracked everywhere, at all times – in other words, a police state dream along with other pervasive spying tools.

Even worse would be mandating human RFID chip implants. It's not planned so far (but not ruled out), and three states (California, Wisconsin and North Dakota) preemptively banned the practice without recipients' consent.

Think it can't happen? Consider a January 13 article in the London Independent headlined "Prisoners 'to be chipped like dogs.' " The article states that civil rights groups and

probation officers are furious that “hi-tech ‘satellite’…. machine-readable (microchip) tagging (is) planned (for thousands of offenders) to create more space in jails.” Unlike ankle bracelets now sometimes used, tiny RFID chips would be surgically implanted for monitoring the way they’re currently used for dogs, cats, cattle and luggage. They’re more reliable, it’s believed, as current devices can be tampered with or removed.

Ken Jones, president of the Association of Chief Police Officers (ACPO), was quoted saying: “We have looked at….the practicalities and the ethics (and we concluded) its time has come.” The UK currently has the largest prison population per capita in western Europe. It sounds like authorities plan to expand it using fewer cells. It also sounds like a scheme to tag everyone after testing them first on prisoners. And consider the possibilities. RFID technology is advancing, and one company plans deeper implants that can vibrate, emit electroshocks, broadcast a message to the implantee, and/or be a hidden microphone to transmit conversations. It’s not science fiction, and what’s planned for the UK will likely come to America. In fact, it’s already here.

In 2004, the FDA approved a grain-of-rice sized, antenna-containing VeriChip for human implantation that allows vital information to be read when a person’s body is scanned. The company states on its web site that it’s “the world’s first and only patented, FDA-cleared, human-implantable RFID microchip….with skin-sensing capabilities.” Reportedly, about 2000 test subjects now have them, but it may signal mandatory implantation ahead. Consider for whom for starters – prisoners, military personnel and possibly anyone seeking employment. After them, maybe everyone in a brave new global surveillance world.

It gets worse. Katherine Albrecht authored a report called “Microchip-Cancer Report – Microchip-Induced Tumors in Laboratory Rodents and Dogs: A Review of the Literature 1990-2006.” After reading it, Dr. Robert Benezra, Director Cancer Biology, Genetics Program, Memorial Sloan-Kettering Cancer Center said: “There’s no way in the world, having read this information, that I would have one of those chips implanted in my skin, or in one of my family members. Given the preliminary animal data, it looks to me that there’s definitely cause for concern.”

Albrecht’s report evaluated 11 previously published toxicology and pathology studies. In six of them, up to 10.2% of rats and mice developed malignant tumors (typically sarcomas) where microchips were implanted. Two others reported the same findings for dogs. These tumors spread fast and “often led to the death of the afflicted animals. In many cases, the tumors metastasized and spread to other parts of the animals. The implants were unequivocally identified as the cause of the cancers.”

Report reviews, conclusions and recommendations were to immediately stop further human implantations, inform people with them of the dangers, offer a microchip removal procedure, and reverse all animal microchipping mandates.

Debate Ahead on New DHS ID Rules

DHS Secretary Michael Chertoff said new ID rules require states to verify each cardholder’s personal information (including a person’s legal status in the country) by matching it against federal Social Security and passport databases and/or comparable state ones.

States have time to adjust, but Senate Judiciary Chairman Patrick Leahy wasted no time saying he’ll recommend legislation to ban Real ID drivers’ license provisions because “so

many Americans oppose" them. They're intrusive, burdensome, and federal databases are full of false or out-of-date information that's hard to disprove, but unless it is Americans will be denied their legal right to a driver's license.

The ACLU also strongly opposes Real ID because it violates privacy, lets government agencies share data, and its "tortured remains" represent an "utterly unworkable" system that will "irreparably damage the fabric of American life." An ACLU January 11 press release further states that DHS "dumped the problems of the statute on future presidents like a rotting corpse left on (its) steps (and) whoever is president in 2018." Congress must "recognize the situation and take action." The Real ID Act and new DHS rules must be "repealed and replaced with a clean, simple, and vigorous new driver's license security law that does not create a national ID" or violate Americans' privacy.

Futuristic Hi-Tech Profiling

On January 14, Computerworld online revealed more cause for concern in an article called "Big Brother Really is Watching." It's about DHS "bankrolling futuristic profiling technology…." for its Project Hostile Intent. It, in turn, is part of a broader initiative called the Future Attribute Screening Technologies Mobile Module. It's to be a self-contained, automated screening system that's portable and easy to implement, and DHS hopes to test it at airports in 2010 and deploy it (if it works) by 2012 at airports, border checkpoints, other points of entry and other security-related areas.

Here's the problem. If developed (reliable or not), these devices will use video, audio, laser and infrared sensors to feed real-time data into a computer using "specially developed algorithms" to identify "suspicious people." It would work (in theory) by interpreting gestures, facial expressions and speech variations as well as measure body temperature, heart and respiration rate, blood pressure, skin moisture, and other physiological characteristics.

The idea would be detect deception and identify suspicious people for aggressive interrogation, searches and even arrest. But consider what's coming. If developed, the technology may be used anywhere by government or the private sector for airport or other checkpoint security, buildings, job interviews, employee screening, buying insurance or conducting any other type essential business.

Aside from Fourth Amendment issues, here's the problem according to Bruce Schneier, chief technology officer at security consultant BT Counterpane: "It's a good idea fraught with difficulties….don't hold your breath" it will work, and a better idea is to focus on detecting suspicious objects. Schneier further compares the technology to lie detectors that rely on "fake technology" and only work in films. They're used because people want them although it's acknowledged, even when well-administered, their median accuracy percentage is 50% at best.

This technology is worse, it may never be reliable, but may be deployed anyway in the age of "terror." Something to consider next time we blink going through airport security, and ACLU Technology and Liberty Project director Barry Steinhardt states the concern: "We are not going to catch any terrorists (with it), but a lot of innocent people, especially racial and ethnic minorities, are going to be trapped in a web of suspicion." Even so, DHS spent billions on this and other screening tools post-9/11. Expect lots more ahead, and here's the bottom line:

As things now stand, Washington, post-9/11, suspended constitutional protections in the name of national security and suppressed our civil liberties for our own good. This article reviewed their newest tools and wonders what's next. This writer called it Police State America in December that won't change with a new White House occupant in 2009 unless organized resistance stops it. Complacency is unthinkable, and unless we act, we'll deserve Aleksandr Herzen's curse of another era – to be the "disease," not the "doctors."

Stephen Lendman is Research Associate of the Centre for Research on Globalization (CRG). He lives in Chicago and can be reached at lendmanstephen@sbcglobal.net.

Also visit his blog site at *www.sjlendman.blogspot.com*.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Stephen Lendman**

About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III." http://www.claritypress.com/LendmanIII.html Visit his blog site at sjlendman.blogspot.com. Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.