GlobalResearch
Center for Research on Globalization

"Big Brother" Presidential Directive: "Biometrics for Identification and Screening to Enhance National Security"

By Prof Michel Chossudovsky
Global Research, June 11, 2008
11 June 2008

Region: USA
Theme: Police State & Civil Rights

The latest Big Brother police state measure emanating from the Bush administration, with virtually no press coverage, is NSPD 59 (HSPD 24) entitled **Biometrics for Identification and Screening to Enhance National Security** [Complete text of NSPD 59 (HSPD 24) in Annex below]

NSPD is directed against US citizens.

It is adopted without public debate or Congressional approval. Its relevant procedures have far-reaching implications.

NSPD 59 goes far beyond the issue of biometric identification, it recommends the collection and storage of *"associated biographic"* information, meaning information on the private lives of US citizens, in minute detail, all of which will be "accomplished within the law":

> "The contextual data that accompanies biometric data includes information on date and place of birth, citizenship, current address and address history, current employment and employment history, current phone numbers and phone number history, use of government services and tax filings. Other contextual data may include bank account and credit card histories, plus criminal database records on a local, state and federal level. The database also could include legal judgments or other public records documenting involvement in legal disputes, child custody records and marriage or divorce records."(See Jerome Corsi, June 2008)

The directive uses 9/11 as an all encompassing justification to wage a witch hunt against dissenting citizens, establishing at the same time an atmosphere of fear and intimidation across the land.

It also calls for the integration of various data banks as well as inter-agency cooperation in the sharing of information, with a view to eventually centralizing the information on American citizens.

In a carefully worded text, NSPD 59 *"establishes a framework"* to enable the Federal government and its various police and intelligence agencies to: *"use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under*

United States law."

The Directive recommends: "actions and associated timelines for enhancing the existing terrorist-oriented identification and screening processes by expanding the use of biometrics".

"Other Categories of Individuals"

The stated intent of NSPD 59 is to protect America from terrorists, but in fact the terms of reference include any person who is deemed to pose a threat to the Homeland. The government requires the ability:

> "to positively identify those individuals who may do harm to Americans and the Nation... Since September 11, 2001, agencies have made considerable progress in securing the Nation through the integration, maintenance, and sharing of information used to identify persons who may pose a threat to national security.

The Directive is not limited to KSTs, which in Homeland Security jargon stands for *"Known and Suspected Terrorists":*

> "The executive branch has developed an integrated screening capability to protect the Nation against "known and suspected terrorists" (KSTs). The executive branch shall build upon this success, in accordance with this directive, by enhancing its capability to collect, store, use, analyze, and share biometrics to identify and screen KSTs and other persons who may pose a threat to national security.
>
> The executive branch recognizes the need for a layered approach to identification and screening of individuals, as no single mechanism is sufficient. For example, while existing name-based screening procedures are beneficial, application of biometric technologies, where appropriate, improve the executive branch's ability to identify and screen for persons who may pose a national security threat. To be most effective, national security identification and screening systems will require timely access to the most accurate and most complete biometric, biographic, and related data that are, or can be, made available throughout the executive branch."

NSPD 59 calls for extending the definition of terrorists to include other categories of individuals "who may pose a threat to national security".

In this regard, it is worth noting that in the 2005 TOPOFF (Top officials) anti-terror drills, two other categories of individuals were identified as potential threats: "Radical groups" and "disgruntled employees", suggesting than any form of dissent directed against Big Brother will be categorized as a threat to America.

In a previous 2004 report of the Homeland Security Council entitled Planning Scenarios, the enemy was referred to as the Universal Adversary (UA).

The Universal Adversary was identified in the scenarios as an abstract entity used for the purposes of simulation. Yet upon more careful examination, this Universal Adversary was by no means illusory. It included the following categories of potential "conspirators":

"foreign [Islamic] terrorists" ,

"domestic radical groups", [antiwar and civil rights groups]

"state sponsored adversaries" ["rogue states", "unstable nations"]

"disgruntled employees" [labor and union activists].

According to the DHS Planning Scenarios Report :

> "Because the attacks could be caused by foreign terrorists; domestic radical groups; state sponsored adversaries; or in some cases, disgruntled employees, the perpetrator has been named, the Universal Adversary (UA). The focus of the scenarios is on response capabilities and needs, not threat-based prevention activities." (See Planning Scenarios)

Under NSPD 59, biometrics and associated biographical information will be used to control all forms of social dissent.

Domestic radical groups and labor activists envisaged in various counter terrorism exercises, constitute in the eyes of the Bush administration, a threat to the established economic and political order.

In the text of NSPD 59, these other categories of people have been conveniently lumped together with the KSTs ("known and suspected terrorists"), confirming that the so-called anti-terror laws together with the Big Brother law enforcement apparatus and its associated data banks of biometric and biographic information on US citizens are intended to be used against all potential domestic "adversaries" including those who oppose the US led war in the Middle East and the derogation of the Rule of Law in America.

It is worth noting that NSPD 59 was issued on June 5, 2008, 4 days prior to the publication of Rep. Dennis Kucinich's Articles of Impeachment of President George W. Bush by the House of Representatives. Article XXIII of the Articles Impeachment underscore how in derogation of the Posse Comitatus Act, which prevents the military from intervening in civilian law enforcement, President Bush:

> "a) has used military forces for law enforcement purposes on U.S. border patrol;
>
> b) has established a program to use military personnel for surveillance and information on criminal activities;
>
> c) is using military espionage equipment to collect intelligence information for law enforcement use on civilians within the United States"

In Article XXIV the president is accused on *Spying on American Ctizens without a court-Ordered Warrant , In Violation of the Law and the Fourth Amendment.*

ANNEX

Biometrics for Identification and Screening to Enhance National Security [Complete text of NSPD 59 (HSPD 24) in Annex below]

National Security Presidential Directive and Homeland Security Presidential Directive

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD — 59
HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD — 24

SUBJECT: Biometrics for Identification and Screening to Enhance National Security

Purpose

This directive establishes a framework to ensure that Federal executive departments and agencies (agencies) use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.

Scope

(1) The executive branch has developed an integrated screening capability to protect the Nation against "known and suspected terrorists" (KSTs). The executive branch shall build upon this success, in accordance with this directive, by enhancing its capability to collect, store, use, analyze, and share biometrics to identify and screen KSTs and other persons who may pose a threat to national security.

(2) Existing law determines under what circumstances an individual's biometric and biographic information can be collected. This directive requires agencies to use, in a more coordinated and efficient manner, all biometric information associated with persons who may pose a threat to national security, consistent with applicable law, including those laws relating to privacy and confidentiality of personal data.

(3) This directive provides a Federal framework for applying existing and emerging biometric technologies to the collection, storage, use, analysis, and sharing of data in identification and screening processes employed by agencies to enhance national security, consistent with applicable law, including information privacy and other legal rights under United States law.

(4) The executive branch recognizes the need for a layered approach to identification and screening of individuals, as no single mechanism is sufficient. For example, while existing name-based screening procedures are beneficial, application of biometric technologies, where appropriate, improve the executive branch's ability to identify and screen for persons who may pose a national security threat. To be most effective, national security identification and screening systems will require timely access to the most accurate and most complete biometric, biographic, and related data that are, or can be, made available throughout the executive branch.

(5) This directive does not impose requirements on State, local, or tribal authorities or on the private sector. It does not provide new authority to agencies for collection, retention, or dissemination of information or for identification and screening activities.

Definitions

(6) In this directive:

(a) "Biometrics" refers to the measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition; examples include fingerprint, face, and iris recognition; and

(b) "Interoperability" refers to the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Background

(7) The ability to positively identify those individuals who may do harm to Americans and the Nation is crucial to protecting the Nation. Since September 11, 2001, agencies have made considerable progress in securing the Nation through the integration, maintenance, and sharing of information used to identify persons who may pose a threat to national security.

(8) Many agencies already collect biographic and biometric information in their identification and screening processes. With improvements in biometric technologies, and in light of its demonstrated value as a tool to protect national security, it is important to ensure agencies use compatible
methods and procedures in the collection, storage, use, analysis, and sharing of biometric information.

(9) Building upon existing investments in fingerprint recognition and other biometric modalities, agencies are currently strengthening their biometric collection, storage, and matching capabilities as technologies advance and offer new opportunities to meet evolving threats to further enhance national security.

(10) This directive is designed to (a) help ensure a common recognition of the value of using biometrics in identification and screening programs and (b) help achieve objectives described in the following: Executive Order 12881 (Establishment of the National Science and Technology Council); Homeland Security Presidential Directive-6 (HSPD-6) (Integration and Use of Screening Information to Protect Against Terrorism); Executive Order 13354 (National Counterterrorism Center); Homeland Security Presidential Directive-11 (HSPD-11) (Comprehensive Terrorist Related Screening Procedures); Executive Order 13388 (Further Strengthening the Sharing of Terrorism Information to Protect Americans); National Security Presidential Directive-46/Homeland Security Presidential Directive-15 (NSPD-46/HSPD-15) (U.S. Policy and Strategy in the War on Terror); 2005 Information Sharing Guidelines; 2006 National Strategy for Combating Terrorism; 2006 National Strategy to Combat Terrorist Travel; 2007 National Strategy for Homeland Security; 2007 National Strategy for Information Sharing; and 2008 United States Intelligence Community Information Sharing Strategy.

Policy

(11) Through integrated processes and interoperable systems, agencies shall, to the fullest extent permitted by law, make available to other agencies all biometric and associated biographic and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security.

(12) All agencies shall execute this directive in a lawful and appropriate manner, respecting the information privacy and other legal rights of individuals under United States law, maintaining data integrity and security, and protecting intelligence sources, methods, activities, and sensitive law enforcement information.

Policy Coordination

(13) The Assistant to the President for Homeland Security and Counterterrorism, in coordination with the Assistant to the President for National Security Affairs and the Director of the Office of Science and Technology Policy, shall be responsible for interagency policy coordination on all aspects of this directive.

Roles and Responsibilities

(14) Agencies shall undertake the roles and responsibilities herein to the fullest extent permitted by law, consistent with the policy of this directive, including appropriate safeguards for information privacy and other legal rights, and in consultation with State, local, and tribal authorities, where appropriate.

(15) The Attorney General shall:

> (a) Provide legal policy guidance, in coordination with the Secretaries of State, Defense, and Homeland Security and the Director of National Intelligence (DNI), regarding the lawful collection, use, and sharing of biometric and associated biographic and contextual information to enhance national security; and
>
> (b) In coordination with the DNI, ensure that policies and procedures for the consolidated terrorist watchlist maximize the use of all biometric identifiers.

(16) Each of the Secretaries of State, Defense, and Homeland Security, the Attorney General, the DNI, and the heads of other appropriate agencies, shall:

> (a) Develop and implement mutually compatible guidelines for each respective agency for the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information, to the fullest extent practicable, lawful, and necessary to protect national security;
>
> (b) Maintain and enhance interoperability among agency biometric and associated biographic systems, by utilizing common information technology and data standards, protocols, and interfaces;
>
> (c) Ensure compliance with laws, policies, and procedures respecting information privacy, other legal rights, and information security;
>
> (d) Establish objectives, priorities, and guidance to ensure timely and effective

tasking, collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information among authorized agencies;

(e) Program for and budget sufficient resources to support the development, operation, maintenance, and upgrade of biometric capabilities consistent with this directive and with such instructions as the Director of the Office of Management and Budget may provide; and

(f) Ensure that biometric and associated biographic and contextual information on KSTs is provided to the National Counterterrorism Center and, as appropriate, to the Terrorist Screening Center.

(17) The Secretary of State, in coordination with the Secretaries of Defense and Homeland Security, the Attorney General, and the DNI, shall coordinate the sharing of biometric and associated biographic and contextual information with foreign partners in accordance with applicable law, including international obligations undertaken by the United States.

(18) The Director of the Office of Science and Technology Policy, through the National Science and Technology Council (NSTC), shall coordinate executive branch biometric science and technology policy, including biometric standards and necessary research, development, and conformance testing programs. Recommended executive branch biometric standards are contained in the Registry of United States Government

Recommended Biometric Standards and shall be updated via the NSTC Subcommittee on Biometrics and Identity Management.

Implementation

(19) Within 90 days of the date of this directive, the Attorney General, in coordination with the Secretaries of State, Defense, and Homeland Security, the DNI, and the Director of the Office of Science and Technology Policy, shall, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, submit for the President's approval an action plan to implement this directive. The action plan shall do the following:

(a) Recommend actions and associated timelines for enhancing the existing terrorist-oriented identification and screening processes by expanding the use of biometrics;

(b) Consistent with applicable law, (i) recommend categories of individuals in addition to KSTs who may pose a threat to national security, and (ii) set forth cost-effective actions and associated timelines for expanding the collection and use of biometrics to identify and screen for such individuals; and

(c) Identify business processes, technological capabilities, legal authorities, and research and development efforts needed to implement this directive.

(20) Within 1 year of the date of this directive, the Attorney General, in coordination with the Secretaries of State, Defense, and Homeland Security, the DNI, and the heads of other appropriate agencies, shall submit to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, a report on the implementation of this directive and the associated action plan, proposing any necessary additional steps for carrying out the policy of this directive.

Agencies shall provide support for, and promptly respond to, requests made by the Attorney General in furtherance of this report. The Attorney General will thereafter report to the President on the implementation of this directive as the Attorney General deems necessary or when directed by the President.

General Provisions

(21) This directive:

(a) shall be implemented consistent with applicable law, including international obligations undertaken by the United States, and the authorities of agencies, or heads of such agencies, vested by law;

(b) shall not be construed to alter, amend, or revoke any other NSPD or HSPD in effect on the effective date of this directive;

(c) is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable by law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

Michel Chossudovsky *is the author of the international bestseller America's "War on Terrorism" Global Research, 2005.*

To order Chossudovsky's book America's "War on Terrorism", click here

---

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Prof Michel Chossudovsky

About the author:

Michel Chossudovsky is an award-winning author, Professor of Economics (emeritus) at the University of Ottawa, Founder and Director of the Centre for Research on Globalization (CRG), Montreal, Editor of Global Research. He has taught as visiting professor in Western Europe, Southeast Asia, the Pacific and Latin America. He has served as economic adviser to governments of developing countries and has acted as a consultant for several international organizations. He

is the author of 13 books. He is a contributor to the Encyclopaedia Britannica. His writings have been published in more than twenty languages. In 2014, he was awarded the Gold Medal for Merit of the Republic of Serbia for his writings on NATO's war of aggression against Yugoslavia. He can be reached at crgeditor@yahoo.com