WASHINGTON
LEGISLATIVE OFFICE

October 26, 2012

The Privacy and Civil Liberties Oversight Board
c/o Matthew B. Conrad
Agency Liaison Division
U.S. General Services Administration
Matthew.conrad@gsa.gov

Re: Notice PCLOB-2012-01; Docket No. 2012-0013;
Sequence No. 1

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

Dear Privacy and Civil Liberties Oversight Board Members,

Thank you for the opportunity to provide our views regarding the issues the Privacy and Civil Liberties Oversight Board should include in its forthcoming agenda, and to address the Board at the public meeting on October 30, 2012. Legislative Counsel Michelle Richardson will present our recommendations at the meeting.

The American Civil Liberties Union (ACLU) is a non-partisan civil liberties organization with more than a half million members, countless additional activists and supporters, and 53 affiliates nationwide, dedicated to the principles of individual liberty and justice guaranteed in the U.S. Constitution. The ACLU has been at the forefront of protecting privacy and civil rights from government encroachment for more than 90 years, and we welcome the increased oversight that the Board can provide to executive branch actions undertaken in the name of national security, and too often hidden from public accountability under an impenetrable shroud of secrecy.

There are, unfortunately, many new and existing national defense, homeland security, intelligence and law enforcement programs and

authorities that threaten privacy and civil liberties and lack effective oversight or accountability measures to prevent abuse, deserving of investigation by the Board. We provide below a list of new and emerging programs that appear to expand significantly the government's power to collect and exploit private, personal information about people not even suspected of posing a national security or criminal threat, for inclusion in intelligence and law enforcement databases. In particular, we urge the Board to focus on programs that improperly target people based on activities protected under the First Amendment and/or based on their race, religion, ethnicity and national origin. Such programs raise vital privacy and civil liberties issues that badly need attention from an independent oversight body.

As an initial matter, we urge you to consider one issue that has not received attention commensurate with its impact on Americans' privacy. The Board could have a real and immediate impact by investigating program activities under the amended National Counterterrorism Center (NCTC) guidelines signed by Attorney General Eric Holder and Director of National Intelligence James Clapper in March 2012.[1] These new guidelines authorize collection authorities on a scale not claimed since Congress de-funded the Total Information Awareness program.

Under the original 2008 guidelines, NCTC, being an element of the intelligence community, was properly limited in its authority to collect and retain information about United States persons (American citizens and legal residents) who were not suspected of involvement with terrorism.[2] If the NCTC collected information about US persons not related to terrorism, it was treated as a mistake that had to be identified and corrected by purging such information from NCTC databases within 180 days. This requirement served as a check on the NCTC's domestic activities, and a necessary protection of innocent Americans' privacy.

Under the 2012 guidelines, however, NCTC can now intentionally collect non-terrorism related US person information , and that information can be "retained and continually assessed" for five years.[3] NCTC can now target any U.S. government databases for ingestion based simply on the NCTC Director's determination that it contains "significant terrorism information," which the guidelines do not define. And it can do so regardless of the amount of non-terrorism related US person information NCTC would also sweep in. While NCTC previously claimed authority to ingest entire databases, the retention limits on collection for US persons meant that only datasets consisting almost entirely of terrorism information and/or non-US person information could reasonably be collected using this methodology. By allowing collection and retention of non-terrorism related US person information for five years, the NCTC Guidelines have authorized the NCTC to ingest many new federal databases that consist substantially, or even primarily of non-terrorism related US person information.

The 2012 guidelines do not properly limit the NCTC's uses of this information, so innocent US persons whose information is collected through the NCTC's bulk collection program can be disseminated broadly, even for a host of non-terrorism purposes. NCTC can share with not just federal, state, local or tribal law enforcement, but also foreign entities, and even with individuals or entities that are not part of a government.[4] The new guidelines also specifically authorize NCTC to conduct pattern-based data mining, which has been thoroughly discredited as a useful tool for identifying terrorists. As long as its queries are designed solely to identify information that is reasonably believed to constitute terrorism information, the guidelines authorize NCTC to conduct queries that involve non-terrorism data points and pattern-based searches and analysis (data mining).[5] Data mining searches are notoriously inaccurate and prone to false positives, and it is therefore very likely that individuals with no connection to terrorism will be caught up in terrorism investigations if this technique is used. As far back as 2008, the National Academy of

Sciences found that data mining for terrorism was scientifically "not feasible" as a methodology, and likely to have significant negative impacts on privacy and civil liberties.[6]

Oversight of these new authorities is limited largely to internal controls. Important oversight bodies such as Congress and the President's Intelligence Oversight Board aren't required to be notified, even of "significant" failures to comply with the guidelines.[7] Additional oversight by the PCLOB is essential to protecting Americans' privacy from this invasive new collection authority.

Other programs need additional oversight as well and include:

- New or expanding Intelligence Community activities focused on domestic collection of US person information, including new cyber-security programs, the proposed expansion of the DNI Information Sharing Environment to include suspicious activity reporting not related to terrorism, and the increasing number of US persons being placed on watch lists, particularly while travelling abroad, preventing return flights to the United States;
- Surveillance and obstruction of activity protected under the First Amendment, including intelligence community and law enforcement surveillance/tracking of protest groups and the FBI's use of aggressive and coordinated raids of activists' homes, and abusing the use of Grand Jury subpoenas to jail activists;
- Racial profiling in law enforcement and intelligence activities, such as the FBI's racial and ethnic mapping program and the Transportation Security Agency's behavioral detection programs;
- The use of new surveillance technologies by federal law enforcement and national security agencies, such as mobile phone data and other location-tracking technologies, unmanned surveillance drones, and databases maintained by commercial data aggregators.

This list should is by no means comprehensive. The pool of programs put in place in the years since 2001 is broad, deep, and alarming.

The nation's security establishment has greatly expanded in scope and power in recent years, and the oversight structures created to oversee these vast agencies are small and inadequate. Aside from Japan and South Korea, the United States is the only advanced-industrial nation that has no privacy and data protection commissioner to enforce its privacy laws. We hope that the PCLOB will embark on its mission quickly and begin filling this oversight vacuum with vigor and energy.

We also hope that the PCLOB will engage in the full spectrum of privacy oversight activities—not only investigating and reviewing government actions to ensure the adequate consideration of privacy and civil liberties interests, but also engaging in pro-active policy leadership, providing broad public guidance on how privacy and other civil liberties interests should be protected as our security agencies make use of new technologies.

Thank you for the opportunity to provide this information, and we look forward to working with the Board as it undertakes its crucial mission of protecting American values and privacy.

Sincerely,

Michael Macleod Ball
Washington Legislative Office
Chief of Staff

Michelle Richardson
Legislative Counsel

[1] National Counterterrorism Center, GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION, Released March 22, 2012; For a redline showing the changes created by the new guidelines please see: http://www.aclu.org/files/assets/2008_guidelines_nctc_redlined_with_2012_changes.pdf

[2] MEMORANDUM OF AGREEMENT BETWEEN THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE ON GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER OF TERRORISM INFORMATION CONTAINED WITHIN DATASETS IDENTIFIED AS INCLUDING NON- TERRORISM INFORMATION AND INFORMATION PERTAINING EXCLUSIVELY TO DOMESTIC TERRORISM, October 2008.

[3] 2012 Guidelines at 9.

[4] Id at 13-14.

[5] *Id* at 10.

[6] *See* National Academy of Sciences report, "Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment" http://books.nap.edu/catalog.php?record_id=12452#toc

[7] 2012 Guidelines at 17.