PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
31 October – Public Meeting Submissions

**1.** Shahid Buttar
Executive Director
Bill of Rights Defense Committee

The subject matter I'd like to address includes:

The NSA's dragnet warrantless wiretapping scheme.
The looming specter of indefinite domestic military detention authorized by the NDAA.
The FBI's resurrection of COINTELPRO, and the DOJ's assertion of the state secrets privilege to insulate it.
The proliferation of domestic surveillance abuses coordinated by DHS funded fusion centers.
The particularly egregious surveillance abuses committed by the NYPD.

I'd be happy to address these issues within the 10 minutes provided for speakers addressing the Board. To the extent the time allotted needs ultimately to be diminished, I'd be happy to submit a written statement for the record.

Is it permissible for attendees to videotape the session, or at least our own comments to the Board?

**2.** Steven Aftergood
Federation of American Scientists
1725 DeSales Street NW, Suite 600
Washington, DC 20036
email: saftergood@fas.org
voice: (202)454-4691
web: www.fas.org/sgp

I would like to submit the attached written statement for the upcoming meeting of the Privacy and Civil Liberties Oversight Board. The statement, attached as a PDF file, proposes an agenda item for the Board's consideration. (SEE ATTACHED)

Will not be able to attend in person.

**3.** Cecilia Anastos
Strategic Intelligence, MA
Chief Intelligence Analyst/Instructor
OSINT and Cybercrime Specialist
Private Investigator (VA)
Meta Enterprises, LLC
W: 619-786-6382C: 619-929-4025

Although I will not be able to attend the GSA's 30 OCT meeting in person, I would like to bring this issue to your attention hoping that you can present it to the meeting on my behalf.

The issue concerns the lack of control over the flow of personal information in the cyberspace domain that US citizens currently have. Since 2011, there have been an explosion of companies like Spokeo, MyLife, and many others, that gather, store, mine, combine and recombine (often inaccurately), exchange and sell information about US citizens. This has enabled a proliferation of cybercrime based on the easiness to mount social engineering attacks, cyberstaling, online fraud, etc., and it has eroded in part the Fourth Amendment right of every citizen. [(Note that "many scholars now agree that the Fourth Amendment also provides legal grounds for a right to privacy protection from nongovernmental intrusion." (Tavani, 2011)]

Although one can argue that this information is publicly available, one should question the right of companies to create a complete profile of an individual and make it accessible to all (marketers and criminals). Moreover, the issue of inaccuracy of information as a violation of one's privacy is of most concern. I have found sites where my life have been aggregated and the only accurate information is that I have so far lived in CA and VA. Some of these sites even list unknown individuals claiming that they are my relatives. Should one of them gets into trouble with the law, I would probably receive the uninvited visit of law enforcement personnel and the mainstream media eager to connect dots without doing analysis. We have seen this mistake done during the tragic shooting in Aurora, CO where the media accused a Tea Party member who happened to have the same name of the shooter.

This is affecting our nation at large; this uncontrollable aggregation of personal data is putting at risk police officers and military personnel, as well as civilians. The European Union's Data Protection Directive has a provision that prohibits this massive aggregation of personal information.

In my humble opinion, we urgently need a law that prohibits this practice once and for all; or a midway compromise where one can click on a link and permanently delete the aggregated record. The authorization to aggregate one's records should be an "opt-in" like function; rather than an "opt-out." Although some sites like MyLife.com state that one can do so, it requires notarized documents, and providing Driver's License information and SSN numbers which turns out to be a double-violation of security and privacy.

**4.** Sharon Bradford Franklin
Senior Counsel
The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
202-580-6928 (direct)
202-580-6920 (main)
202-580-6929 (fax)
sfranklin@constitutionproject.org

Please find attached The Constitution Project's statement for the record in connection with the October 30, 2012 public meeting of the Privacy and Civil Liberties Oversight Board.

In addition, I request to be added to the list of individuals addressing the October 30th meeting in person. My full name, title and contact information appear in the signature block below. My oral presentation will be similar in substance to the attached written comments. In summary, TCP urges the PCLOB to focus its attention on the following three priority areas where independent review and oversight are most urgently needed: (1) programs whose very existence is classified and that remain largely if not entirely unknown to the public; (2) the targeted killing or drone program; and (3) programs that involve intelligence collection on, and government monitoring of, U.S. persons and their personal information. This final category is a broad one, ranging from surveillance conducted under the Foreign Intelligence Surveillance Act (FISA) Amendments Act to data mining programs.

I would appreciate it if you would confirm that you have received our statement and my request to make an oral presentation. Thank you.

**5.** Name: Carole Williams
Title: Intern
Organization: Dept of Treasury, Office of Privacy, Transparency and Records and
My attendance would be mere observation, no presentation.

I will attend this Board Meeting on behalf of my office (but not make any oral presentation).

**6.** Gregory T. Nojeim
Senior Counsel and
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology
1634 Eye St., NW Ste 1100
Washington, DC 20006
202.407.8833 direct
202.637.0968 fax
gnojeim@cdt.org

Attached is a request to address PCLOB at its Oct. 30 meeting.

**7.** Michael Price
Counsel, Liberty & National Security Program
Brennan Center for Justice
161 Avenue of the Americas, 12th Floor
New York, NY 10013
(646) 292-8335
michael.price@nyu.edu

On behalf of the Brennan Center for Justice at NYU School of Law, I hereby submit our organization's written statement pursuant to the Notice of Meeting published in the Federal Register on October 23, 2012, at 77 FR 64835.

The Brennan Center also wishes to address the PCLOB meeting orally. Elizabeth Goitein, Co-Director of the Brennan Center's Liberty and National Security Program, would like to speak on our behalf. Ms. Goitein plans to highlight aspects of the Brennan Center's written statement concerning religious profiling, information privacy, and transparency issues.

**8.** Michelle Richardson, Legislative Counsel
American Civil Liberties Union
mrichardson@dcaclu.org
202-715-0825

Attached is the ACLU's written statement for the record of the PCLOB meeting on October 30. I'm also requesting an opportunity to address the panel if time permits. Per our letter, I would suggest the PCLOB look into four areas: 1) new or expanding areas of domestic intelligence collection, 2) surveillance and/or obstruction of First Amendment activity, 3) racial profiling and 4) the use of new technologies that impact privacy. In particular, I'd like to discuss the recent amendments to the National Counter Terrorism Center guidelines as an example.

We very much look forward to working with the PCLOB and hope to be a resource as you move forward.

**9.** Sue Udry
Executive Director
Defending Dissent Foundation
6930 Carroll Ave. Suite 413
Takoma Park, MD 20912
www.defendingdissent.org
twitter: @defenddissent
office: 202-529-4225; cell: 301-325-1201
Attached please find my statement for the record for Tuesday's PCLOB meeting.

**10.** Ian Churchill
Program Associate
Center for National Security Studies
1730 Pennsylvania Ave NW, 7th Floor
Washington, DC 20006
P: 202-721-5650
F: 202-530-0128
Attached is a request from Kate Martin, Director of the Center for National Security Studies to address the Privacy and Civil Liberties Oversight Board on October 30, 2012.

**11.** Gavin Baker
Federal Information Policy Analyst
OMB Watch
gbaker@ombwatch.org
Phone: (202) 683-4834
Twitter: @opengavin

LinkedIn: gavinrbaker
Please see attached a written statement for the record for the Privacy and Civil Liberties Oversight Board's upcoming public meeting.

**12.** Sam Jewler
sam.jewler@gmail.com
I'd like to submit this testimony and register to present it orally at Tuesday's hearing. (See attachment)

**13.** Julian Sanchez
Research Fellow
Cato Institute
1000 Massachusetts Ave NW
Washington, DC 20001
Ph: 202/789.5243
Cell: 917/318.3631
Skype: normative
I'd like to be placed on the schedule to address next week's PCLOB meeting if possible.
I intend to make one broad general point, and then highlight a few specific items for consideration. The general point is that, given the nature of the civil liberties issues we've seen arise historically with intelligence surveillance, the board should not assume that its limited ability to review classified information will enable it to identify the most serious potential problems with any specificity, but instead adopt an architectural approach. They should, for example, not simply ask which procedures would provide better safeguards, but ask which system architectures will generate the least damaging consequences in the event of an undetected violation of those procedures. One implication is that the board should be on the lookout for any collection program that does not appear to be generating unique and valuable intelligence, on the premise that any privacy risk without demonstrable benefit is, by definition, excessive whether or not any current problems are apparent. More specifically, I'll suggest a handful of areas where there's reason to believe that the collection of private information may be wildly disproportionate to the amount of useful *intelligence* information gathered, and suggest the board evaluate privacy concerns there through this kind of cost benefit lens: FAA/702 surveillance programs; the use of National Security Letters in preliminary investigations, and possible use of 215 for bulk records acquisition—potentially including geolocation tracking.

As my under-the-wire e-mail may suggest, I haven't had time to write up my remarks for inclusion in the record yet, but would gladly send them along over the weekend if that wouldn't be too late.

**14.** Kyle Lennox
(315) 380-9851

Attached is a document pertaining to citizens Privacy and Civil Liberties that is to be indexed by the Privacy and Civil Liberties Board.