The public meeting was held at the JW Marriott Hotel, 1331 Pennsylvania Avenue NW, Washington, D.C. 20004, commencing at 1:05 p.m.

Reported by: Lynne Livingston
BOARD MEMBERS

David Medine, Chairman
Rachel Brand
Patricia Wald
James Dempsey
Elizabeth Collins Cook

Public Comments

Shahid Buttar, Executive Director, Bill of Rights Defense Committee
Tom Devine, Legal Director, Government Accountability Project
Robert S. McCaw, Government Affairs Manager, Council on American-Islamic Relations (CAIR)
Gregory T. Nojeim, Director, Project on Freedom, Security & Technology, Center for Democracy and Technology (CDT)
Jeramie Scott, National Security Counsel, Electronic Privacy Information Center (EPIC)
John Napier Tye, Legal Director, Avaaz, formerly Section Chief for Internet Freedom in the Bureau of Democracy, Human Rights and Labor, U.S.
Department of State
PROCEEDINGS

MR. MEDINE: Good afternoon. This is a meeting of the Privacy and Civil Liberties Oversight Board. It is 1:05 p.m. The date is July 23, 2014. We're at the JW Marriott Hotel at 1331 Pennsylvania Avenue NW, Washington, D.C.

This meeting was announced in the Federal Register on July 9th, 2014, and as Chairman, I will be the presiding officer. All five Board members are present and there is a quorum.

I now call meeting to order. All in favor of opening the meeting say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent to proceed, we will now proceed.

There are three item of business for today's meeting. The first is to vote on the Board's semiannual report. The second is to announce the Board's short-term agenda of projects, and the third is to receive public input.
There are a number of people who submitted a request to speak at this meeting with regard to suggestions about the Board's midterm and long-term agenda.

So the first order of business is the Board's semiannual report. The report covers the period from September 2013 through March 2014, and addresses the statutory requirement that the Board report no less than twice a year to the President and Congress.

The report summarizes the Board's activities during that period, including the completion of it's 215 Report and the substantial work it had done as of then on the 702 Report, which of course was issued on July 2nd.

It also discusses the consultation the Board has had with the Department of Homeland Security on cybersecurity, their cybersecurity report, and notes the increase in the Board's staff, and for the development of its website.

There is information on the Board's findings, conclusions, and recommendations.
resulting from its oversight and advice functions, as well as minority views on any findings, conclusions, and recommendations of the Board resulting from its oversight and advice.

Unless there's any comment or discussion, I would move the adoption of the semiannual report. All in favor of adopting the report say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent to adopt the report, the report is now final. Copies are available in the room and copies are also available online later at the Board's website, www.pclob.gov.

Moving on to the next agenda item is the Board's short-term agenda of projects. The list that I'm about to go through of projects is not the only things the Board is working on. The Board is also considering other matters that are still in progress in terms of the Board's consideration of what to proceed on.

And also, I'm not giving a list in order
of importance. It's simply a list of the activities the Board plans on engaging in, in the short-term now that the Board has completed its 215 and 702 reports.

The first thing I'm going to mention is PPD-28. On January 17th of this year, President Obama signed the Presidential Policy Directive 28 on Signals Intelligence, which addresses the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws.

The President encouraged our Board to provide him with a report that assesses the implementation of any matters contained within the directive that fall within the Board's mandate.

During the coming year, the Board will be assessing the PPD-28 implementation and providing a report to the President, as requested.

Next is training. It's one thing for the government to have good policies but if they
don't get translated into action and awareness by the people on the front lines, they're not as meaningful as they should be, particularly in the area of privacy and civil liberties, and so training is a key connection between policy and implementation.

And so the Board has reached out to the intelligence community to develop an inventory of training materials and to better understand how those materials are being utilized.

So the Board will continue to work with the intelligence community to ensure that training on privacy and civil liberties is effective.

Next is cybersecurity. Cyber attacks continue to pose a threat to both the private sector and the government. The President's Executive Order on Cybersecurity, issued on February 12th of last year, called for the agencies involved, including Homeland Security and the Department of Justice, to conduct assessments of those agencies' activities and
provide those assessments to the Department of Homeland Security for annual report.

The agencies are to consider the assessments and recommendations in that report in implementing their privacy and civil liberties protections with regard to cybersecurity.

The executive order calls for the Department of Homeland Security's Privacy and Civil Liberties offices to consult with the Privacy and Civil Liberties Oversight Board regarding the report, and during the coming year the Board looks forward to working with the Department of Homeland Security and the other agencies involved in the cyber report.

Next is, what is privacy. As a Privacy and Civil Liberties Oversight Board one of the fundamental issues that we have to address is what is privacy, for purposes of balancing privacy and civil liberties with national security.

In the coming months we plan on having a forum in which we seek public input and dialogue
and discussion of what is privacy, particularly in the context of national security and our Board's operations.

And obviously we will announce that and give people an opportunity to comment on it. We think there will be a very productive dialogue.

Executive Order 12333 is next. It establishes the overall framework for the conduct of intelligence activities by the U.S. intelligence agencies. It provides that they can only collect, retain, and disseminate information about U.S. persons if permitted by the agency's attorney general guidelines, something that, before I joined the Board, the Board had identified that some of the attorney general guidelines implementing 12333 were outdated, to say the least, some as many as three decades old, preceding text messaging, and email just getting started.

Obviously there have been dramatic technology changes, not to mention the very substantial debate that's gone on over the past
year on surveillance issues. And so we're going to continue to encourage the updating of those guidelines and offer our advice as part of that process of updating the AG guidelines.

In addition, the Board is also exploring how to approach 12333 more broadly than its current efforts regarding the AG guidelines and we will be considering staff recommendations about how to look at the operations of 12333.

And I believe that some of the speakers later in the program, I think, will also be addressing 12333 issues.

Next is the nationwide Suspicious Activity Reporting, or SAR initiative, which builds on what law enforcement agencies have been doing for years, which is gathering information about behaviors of people who may be associated with criminal activity, and establishes a standardized process whereby that information can be shared among agencies to help detect and prevent counterterrorism.

The Director of National Intelligence
has Information Sharing Environment. The program manager has published functional standards for state and local law enforcement agencies to use to report suspicious activities to fusion centers and to the intelligence community. So we will be evaluating those functional standards' impact on privacy and civil liberties.

Next is efficacy. As noted in our 702 Report, the efficacy of any particular counterterrorism program is very difficult to assess because the programs serve a variety of functions and can be evaluated both on qualitative and quantitative bases.

We will be working with the intelligence community to see if we can develop a methodology for assessing the effectiveness of programs, both in terms of thwarting terrorism, and in terms of whether they're appropriate uses of budget or whether alternative programs would be equally or more effective, particularly with respect to honoring privacy and civil liberties concerns.

And then lastly, the 803 Reports. Eight
federal agencies are required, by statute, to submit to the Privacy and Civil Liberties Oversight Board, for review, quarterly reports on the number of public or internal complaints that they receive, the types of advice and response that resulted, and the nature of complaints and their disposition.

For the most part, the 803 Reports are not particularly informative, as they're mostly quantitative summaries of complaints that were received and not a qualitative evaluation of what those summaries are about, what trends there are in complaints, and the nature of those complaints.

And so the Board has been and will continue to work with the affected agencies and see if there is an approach where we could improve the meaningfulness, the transparency of the 803 Reports so there's a better understanding by the public of what kinds of complaints are being filed with the agencies, what their nature is, and how they're being handled.
The Board also has authority to add to the agencies that are currently 803 reporters, and we will certainly consider whether any agency should be added to the 803 process, particularly if it could be made more meaningful as we move forward.

So I'm ready to move forward with the speakers unless any Board members have any additional comments.

Again, we have invited public comment and six speakers submitted requests to appear.

Is Shahid Buttar here? Thank you. Please have a seat. If you could identify yourself, and for the benefit of the court reporter speak more slowly than I've been speaking so far.


There are a few issues here I just want to expand the context, and I appreciate your expression of the various fronts on which the
Board is investigating intelligence and surveillance practices and the various threats they pose to privacy. I want to expand the context in a few different dimensions.

So the first, just to note, you at one point referenced the debate that's taken place over the last year, in the wake of the Snowden revelations in particular.

Even before it, over the past decades hundreds of American cities and eight states have formally repudiated the very same PATRIOT Act repudiated by its authors in the House and the Senate since the Snowden revelations. So there is a consensus that is long established that these powers are un-American.

I just want to put that on the table to frame the rest, both of my remarks, and to the extent it informs your evaluation of these programs, I think it's an important history not to lose sight of in the conduct of your own mission.

And in that context, the debate that has
happened in the last year has been both long overdue and also very stilted, in the sense that your mission is to investigate an iceberg, the extent of which remains unknown to everyone outside the agencies. Congress has no idea how vast the iceberg is, you don't have any idea how vast the iceberg is, the press certainly doesn't have any idea how vast the iceberg is.

So there's a debate prompted by pinpricks in a blanket of secrecy that persists. And that's the context in which you're operating.

And so I would encourage you not to rely, for instance, on the isolated voices of whistleblowers to give you the very limited instances of transparency that you do have behind an institutional veil of secrecy that, to this point, and for the first ten years of its operation, hid the dragnet from the people who enabled it in Congress even, right?

And even since then, think about the statements of the Director of National Intelligence on the record to Congress. There's
active obfuscation by the executive branch continuing as to the basic facts of the issues that you are charged to oversee. So again, just to frame it there.

With respect to some particular issues, and I think you addressed some of these, but I want to add, particularly to the SAR discussion, and then there were a few zones of surveillance that I don't think it sounded like you were considering yet, but I just want to encourage you to examine.

So the first is the FBI's infiltration and entrapment regime. Multiple reports, including one by the National Coalition to Protect Civil Freedoms have recently established the pattern, I would daresay a modus operandi by the FBI of contriving prosecutions by essentially enabling, particularly terror plots that would never be contemplated by the supposed participants.

HBO has a documentary out, the Newburgh Sting, about one of these particular cases in
1 upstate New York that very vividly tells the tale
2 of a particular example.
3
4 There's also the Fazaga litigation in
5 southern California you might look at as an
6 interesting example of institutional duplicity
7 and repeated lies, even to courts, by FBI agents
8 about the parameters of their investigations, one
9 of which included sexual blackmail by an FBI-sent
10 informant into multiple faith communities in
11 southern California, compounding offense upon
12 offense. And this has never been adequately
13 explored by Congress.
14
15 I could point you to a July 2010 Senate
16 Judiciary Committee hearing where the issue came
17 up in the abstract, both with respect to
18 religious profiling and political profiling. And
19 I'd give you as Exhibit A here would be the
20 Occupy movement.
21
22 There's current litigation and a FOIA
23 suit over the FBI and the Houston police
24 department's possession of an alleged document
25 that authorizes the assassination of nonviolent
political activists.

And I need not remind you of the fracas when Senator Paul resisted the CIA Director's nomination over precisely that issue, the assassination of Americans without trial. And that's something that you should absolutely be examining, I think, and factoring into your assessment of the landscape of these issues beyond the individual trees in that forest.

In the vein of infiltration, beyond the FBI there's a very recent case in the Ninth Circuit that you should examine, the Towery case involving the Pentagon infiltrating nonviolent peace groups. And it's also doubly offensive because it interlaces with the SAR network.

The individual, a civilian Defense Department employee who infiltrated a series of peace groups, was himself an intelligence analyst working in a fusion center as a military representative.

And it demonstrates not only the susceptibility of the infrastructure to being
undermined from within, but also the inability of courts to exercise effective checks in this arena, especially to address prior restraints.

You mentioned suspicious activity reports and the extent to which they've been used potentially as a tool to track political affiliation. There are also further problems with respect particularly to racial and religious profiling that, to my knowledge at least, have never been addressed.

And we've seen historical examples of this dating back to 2008, 2009, involving some of the very same actors that the NSA was recently revealed to have been monitoring in the most recent Snowden leaks and up to the present.

One particular veil of secrecy I referenced before is important to recognize here because the investigations of fusion centers to this point, there have been none that are independent.

The only time that Congress has particularly spoken about this, it was a
bipartisan report out of the Senate that Senator Coburn particularly authored that was very sharply critical of the fusion center network for its abject lack of transparency.

As far as I know, no one has even been able to quantify the amount of money that they cost, and that is, I dare say, egregious, notwithstanding the civil liberties implications.

There is not at all, widely appreciated, an implication of immigration enforcement for the biometric privacy of U.S. citizens. The next generation initiative that the FBI aspires towards building on the back of immigration enforcement, particularly the secure communities initiative, is terrifying quite frankly, and particularly because the immigration debate is frothing at the moment on other dimensions.

This body's examination of its implications for U.S. citizen privacy could add a great deal to the discussion. And I'm happy to point you to more information here.

One liner, even the U.S. Postal Service
is spying on Americans en mass. And I haven't heard that come up yet, but pervasive tracking of metadata extends into snail mail as well.

And just to tie those things together, as you evaluate the state of privacy and civil liberties in the United States and how to protect it, it's worth noting that there is a confluence between a high tech panopticon of the sort that the NSA is exercising through the phone and the Internet dragnets and a low tech Stasi-like sort of surveillance that the FBI and local police departments are implementing through the SAR program and the infiltration regime.

And that is a very dangerous combination, the likes of which has never been seen in human history, and we are flirting with a very dangerous set of implications there.

The last thing I want to offer is a strategy to establish this Board's independence going forward. Your first report on telephony metadata demonstrated a very relieving degree of independence, particularly the legal analysis and
the finding of the illegality of the Section 215 interpretation that multiple senators had alluded to before.

Your second report on 702 was profoundly disappointing. I dare say it bordered on sycophancy. The acceptance of facts from agencies that have already been caught lying to Congress on the public record, and the extent of your investigation, especially when there are whistleblowers out there -- so let's just start there.

The easiest thing you might do is give a microphone to and hear from the many NSA whistleblowers who have tried to brief Congress on multiple occasions. Snowden, obviously would be hard. Thomas Drake lives down the street, right? William Binney, Mark Klein, bring in James Bamford. There are many people who could give you a great deal of insight into the agency, from whom, as far as I know, you have not heard. That would be a very low hanging fruit, you might say, in the efforts to establish the institution.
There's a further opportunity here beyond the whistleblowers to engage the whistleblowers from other agencies. I'm thinking the only one in particular comes to mind off the top of my head is John Kiriakou, who doesn't quite fit because he blew a whistle on torture at the CIA, which is not necessarily within your ambit, as far as I know. If it is, I would encourage you to talk to him.

But think about, for instance, the survivors of institutional assaults, and I have in mind, for instance, there is in many families in the HBO documentary about the Newburgh sting, who have suffered with their loved ones basically being bribed into plots that the FBI initiated. It would be very compelling for this Board to examine them.

And these are people from communities that you might not often think of as implicated by these issues, right, low income, black neighborhoods in bedroom communities in New York, for instance, among others.
There's a very compelling mother of a young, mentally challenged young man who was basically brainwashed by an NYPD agent into saying something stupid that landed him in counterterrorism.

These are the examples, other pinpricks in the veil of secrecy that you might actively avail yourself of.

And the last thing I would just say is not to take the agency's word for what they say and to do what you can to be independent. Thank you.

MR. MEDINE: Thank you for your comments and for keeping right on time, which is ten minutes. So we appreciate that.

Tom Devine? And again, if you could identify yourself and your affiliation.

MR. DEVINE: Pardon?

MR. MEDINE: Identify yourself and who you're with, who you're appearing upon or if you're by yourself.

MR. DEVINE: Oh, yes, I work at the
Government Accountability Project. We're a whistleblower support NGO, nonprofit, nonpartisan.

We've led the campaign, been a leader in campaigns to pass or defend nearly all the federal whistleblower laws since 1978. And my presentation complements Shahid's remarks.

I asked to speak to the Board for the purpose of advocacy to seek protection for whistleblowers and other witnesses who communicate with the Board.

This is not an unprecedented type of move for organizations such as your own. It's based on rights to communicate with Congress safely that have been in place since 1912. It's been on other independent boards and agencies.

In my own experience, the Commission on Research Integrity that I participated in had a rule to protect our witnesses against retaliation. It doesn't require statutory authorization.

For example, the EPA has, through
regulations, whistleblower protection for those
who have to enforce its pesticide program in the
absence of a statutory mandate.

But nearly all whistleblower laws since
2002 covering the private sector have had these
protections.

And Congress just enacted them for
federal workers in the Intelligence Authorization
Act. But that act only protects them for
disclosures within specified internal channels or
to the select committees on intelligence. It
would not give them rights to provide information
to the Board.

Probably the first thing to do, besides
sharing that this isn't a unique precedent, is to
share the justification based on the
whistleblower's role in exposing the issues that
are the Board's mission.

I think our first significant
disclosures of questionable domestic surveillance
came from a corporate whistleblower, Matt Klein
from AT&T, who exposed a channel to the NSA.
A second whistleblower, Babak Pasdar, exposed a Quantico connection where everything on Verizon's system was being forwarded to Quantico, Virginia.

A third whistleblower, Thomas Tamm from the Justice Department, exposed the NSA's domestic surveillance program, Operation Stellar Wind.

Three whistleblowers from the National Security Agency, Thomas Drake, Kirk Wiebe, and Bill Binney, exposed the full scope of unfiltered surveillance in trying to analyze the data and their frustration at attempts to restrict the screening so that it would only be for lawfully entitled information. They completely hit the wall in favor of NSA's system to analyze everything that came in.

And then of course Mr. Snowden's disclosures have sort of taken it beyond the he said, she said debate of the prior dialogue to eliminate the uncertainty that this practice exists.
We would still be flying blind without whistleblowers, and we need them if we're not going to crash into mountains as we continue our journey to deal with this issue. And there's a real justification based on need for them to have some dedicated rights to communicate with the Board.

Currently their rights are limited to, if they exist at all, they're limited to the inspectors general and the select committees on intelligence in Congress. These have not been effective outlets to have a monopoly on disclosures. The IGs have not been responsible, and in fact, have abused their authority to initiate retaliation against the whistleblowers who tried to work within that channel.

In the NSA case, although the three or four whistleblowers, plus a congressional staffer who participated in the NSA and Department of Defense investigations of domestic surveillance, worked through channels, worked through the IG system, donated literally hundreds of hours of
time to work responsibly through proper channels, they were then referred to the Department of Justice as suspects for Mr. Tamm's leak.

All of them enjoyed simultaneous FBI raids of 10 to 20 people at daybreak where their homes were ransacked, their property was widely confiscated and still hasn't been returned. Their families were terrorized.

One, Bill Binney, he said good morning to a pistol pointed at his head in the shower by an FBI agent. This was trying to work through the IG system.

It's not surprising that Mr. Snowden said I'd rather leak than try that approach. It wasn't a trustworthy approach.

The policy perspective of the select intelligence committees in their efforts to, on the House side, eliminate whistleblower rights, or on the Senate side to maximize agency discretion for surveillance, have left them as a remote prospect for whistleblowers to sufficiently trust to open up and communicate
with.

That means that the Board has a unique opportunity to establish an independent, legally safe channel to get this evidence to where it's needed, both in terms of establishing rights and in terms of enforcement.

While you don't have statutory authority to punish people, you can engage in disclosures of retaliation against your witnesses to all the relevant congressional committees, call for briefings by the agencies that are responsible, and pursue oversight of this issue. There can be referrals to the Office of Special Counsel or to the Office of the Director of National Intelligence, OIG, which has a whistleblower ombudsman to deal with the associated retaliation.

And they'd have a much better chance if it were a referral from the Board rather than just knocking on the door and asking for help.

There also could be voluntarily systems to set up arbitration to deal with associated
disputes or questions about what could be disclosed.

While you don't have statutory teeth, there's a lot that this Board can do to protect its witnesses and enhance the free flow of information for your oversight. Thanks for hearing me out.

MR. MEDINE: Thank you, Mr. Devine, for your comments.

Robert McCaw?

MR. DEMPSEY: I just have a question. So really it's to both witnesses and all the witnesses.

Tom, you gave us a lot there. It would be very helpful to get this in writing.

Shahid, please as well, because you threw a lot of cases and so on at us.

It seemed to me that you had there the outlines of what would be a whistleblower, maybe you'd call it protection, but at least a whistleblower response process for the Board.

MR. DEVINE: Yes.
MR. DEMPSEY: So if you could write that up as what would be your view of what would be sort of the ideal that the Board could do, as you say, within our existing authority without statutory change, what should it say, that would be very helpful for us.

MR. DEVINE: I'd be very pleased to write it up and more pleased to follow through working with you and your staff.

MR. MEDINE: Let me just add to Mr. Dempsey's comment. There is already statutory whistleblower protection for those who come to the Privacy and Civil Liberties Oversight Board, and so I'd appreciate any thoughts as to whether you believe that statutory protection is adequate or more protection is needed for whistleblowers.

And then again, sort of more broadly, the record for comments and suggestions about the Board's agenda will stay open until the end of August, I believe. And so for those who didn't submit requests to appear, we'd be very happy and
look forward to receiving any written comments, both of those who appeared and those who did not have the opportunity to appear today.

MR. DEVINE: Thank you. And my analysis will be primarily directed towards enforcement.

MR. MEDINE: Do you have a question?

Okay, thank you very much.

Mr. McCaw, and if you could identify yourself and your organization.

MR. MCCAW: Thank you and good afternoon. My name is Robert McCaw. I am the Government Affairs Department Manager for the Council on American-Islamic Relations, the nation's largest Muslim civil liberties and advocacy organization.

CAIR appreciates this opportunity to address PCLOB and provide its views and recommendations on what civil liberties issues with national security implications the Board should address in its midterm and short-term agenda.

A number of the recommendations I make
here today reflect the civil liberty concerns of post-9/11 affected minority communities, Arabs, South Asians, Sikhs, and Muslim-Americans.

I'm also happy or pleased to hear that the Board is going to take on suspicious activity reports, SARs, and also civil liberty implications of trainings for law enforcement and national security agencies.

So concerning watchlist issues, CAIR recommends PCLOB review DHS and DOJ redress policies and procedures regarding racial and religious profiling and questions at points of entry along the U.S. border by CBP, and U.S. airports by TSA, including inappropriate FBI placement of U.S. citizens on traveler's watchlists, including the no-fly list and the list for secondary security screening selection, SSSS.

CAIR also asks the Board to review numerous reports of the FBI placing American citizens on the no-fly list while they're traveling abroad.
This is a form of extrajudicial exile, often for the purpose of coercing these citizens into submitting to interviews with FBI agents or foreign law enforcement officers while being denied legal counsel.

Just to note, at the time these individuals are also pressured as a means of returning home to become spies on their own religious communities, or informants, if you would.

In June a federal district court judge in Oregon ruled that the no-fly list was unconstitutional in that it violated the due process, the procedural due process rights of those watchlisted by providing no meaningful way to contest their designation.

CAIR strongly recommends PCLOB review these interconnected federal watchlisting issues to provide recommendations to the administration, Congress, DOJ, and DHS on how to adequately develop watchlist redress procedures which satisfy federal court concerns over potential
procedural violations of citizens' due process rights.

Specifically CAIR believes that the federal watchlist system needs to be repaired to ensure that people on the no-fly list and other watchlists are provided notice of the fact that they are on a list, a statement of reasons in sufficient and specific detail to meaningfully challenge their inclusion, and a hearing before a neutral fact-finder at which they can contest the government's evidence against them and present their own.

In the event of adverse decision, these watchlisted people should be entitled to a federal judicial review.

Also, the ability to confirm an individual's designation on such watchlists subsequent to a person's filing for a redress through DHS TRIP or experiencing a watchlist-based deprivation, and allow individuals to challenge the terrorist screening center's listing in federal district court.
directly, and access and review any claims or
evidence used in their designation.

Concerning profiling guidelines, CAIR
recommends that PCLOB review guidelines on the
use of race in federal law enforcement and by
federal law enforcement and national security
agencies.

DOJ and DHS guidelines are supposed to
prohibit profiling but they've been
inappropriately used to target Muslims in
counterterrorism investigations and Latinos for
immigration investigations.

CAIR believes that the DOJ and DHS
should revise existing guidelines banning the use
of racial profiling to include nationality and
religion as protected characteristics, as well as
eliminate any loopholes that permit profiling at
U.S. borders or for reasons of national security.

Such a Board review should also target
the Attorney General guidelines for domestic FBI
operations, the AGG and FBI's domestic
investigations and operation guideline, DIOG,
which permit the FBI to engage in racial and ethnic profiling in certain contexts to initiate investigations and to use intrusive investigative techniques, absent of any suspicion or wrongdoing.

A Board review should also be completed on how these guidelines in DIOG impact law enforcement practices in Muslim communities and others, and could help the Attorney General to better understand the harmful effects of these policies.

Concerning the FBI and NSA spying on Muslim leaders, this past month CAIR joined a broad coalition of 45 organizations led by the ACLU in insisting that President Obama provide a full public accounting of surveillance practices of American Muslim leaders.

According to new revelations by Glenn Greenwald and Murtaza Hussain, CAIR’s own National Executive Director was among those U.S. Muslim leaders reported to be targeted by the FBI and NSA surveillance under FISA.
Also among those leaders spied on was Faisal Gill, an American citizen, U.S. Navy veteran, and former Bush Administration DHS official. Of particular concern, Mr. Gill's nationality was marked unknown on a leaked FISA recapped document.

Addressing FBI and NSA targeting of American Muslim leaders, CAIR stated it was an outrageous continuation of civil rights era surveillance of minority community leadership by government elements who see threats in all patriotic dissent.

CAIR strongly recommends that PCLOB reviews these allegations to ensure that the government surveillance works within the bounds of law and Constitution.

Concerning the blanketed surveillance and entrapment of Muslims, also addressed by Shahid, CAIR fully supports law enforcement counterterrorism training investigations that are based on credible information, carried out to prevent criminal acts of violence and halt
material support to would-be terrorists. CAIR believes that responsible enforcement of counterterrorism programs is what truly keeps America safe.

Since September 11th, the FBI has made preventing the next act of terrorism its biggest priority. Out of its 8.2 billion a year budget, 3.3 billion is spent on counterterrorism operations.

During the last decade the FBI has built a network of 15,000 registered community informants, many who are paid to infiltrate American Muslim communities.

CAIR acknowledges the value of the FBI -- acknowledges the value of FBI sting operations in persecuting individuals who would attempt to do our country harm. However, in recent years a number of troubling details have emerged about some informant-led plots.

According to Mother Jones Magazine, all but three of the last decade's high profile terror plots were informant driven FBI stings
that targeted suspects which had no actual ties
to overseas terrorist groups like Al-Qaeda.

Recent details about some of these cases
have CAIR and many other Muslim community
leaders, civil rights groups, and media
questioning whether most of these FBI stings were
grounded towards preventing operational terrorists
or where were actually cases of financially
motivated informants going to great lengths over
long periods of time to radicalize, enable
unlikely, and at times mentally ill, individuals
to commit acts of scripted terrorism.

CAIR recommends PCLOB to investigate
civil rights groups and media allegations that
the FBI has engaged in unlawful or questionable
practices of entrapment in the American Muslim
community, as well as other religious
communities, politically left and right leaning
movements as well.

I would refer you to Human Rights
Watch's recent report, Illusion of Justice, as
well as the HBO documentary on the Newburgh four
which was recently released.

Concerning bias training by federal law enforcement agents, recent headlines were also made by the NSA's blatant use of -- NSA's blatantly prejudiced use of the Mohammed Raghead as a placeholder in an agency document describing how to properly format surveillance justification.

However, this came as no surprise in light of Wired's 2011 reporting that the FBI and Department of Defense were also using anti-Arab, anti-Muslim training materials.

While most of these materials have since been purged, the effects of such training still linger and CAIR recommends the Board complete a review of DOJ and DHS national security and counterterrorism training programs and materials, like you said earlier you would be doing, used to educate agents and officers on minority communities' cultural beliefs, practices, and in addition to trainings on upholding civil rights and liberties of American citizens and persons
residing in the U.S.

In its review, CAIR suggests PCLOB consider the following reform measures,
standardize educational materials across all departments and agencies about respective minority cultures, beliefs, and practices with involvement from Arab, South Asian, Sikh, and Muslim organizations, and to ensure that the First Amendment protected activities and nonviolent civil disobedience is not improperly equated with terrorism.

Create an ongoing system to ensure that all training materials and intelligence products that contain factually incorrect or biased information continue to be removed from use.

Bar unqualified course instructors who provide biased or inaccurate trainings and hold these individuals accountable.

And call for transparency in how federal national security and counterterrorism training funds, grants are distributed to state and local law enforcement agencies and to which trainers
these funds are provided to.

And finally, to retrain national security and counterterrorism officers and agents who, for the past decade, received such inaccurate or biased instructions.

Finally, I'd just like to discuss issues concerning the fusion centers. CAIR lastly recommends PCLOB review the activities of state and local intelligence fusion centers that receive federal funding or operate under voluntary DOJ or DHS guidelines to determine whether they operate within the law, including regulations governing the collection, retention, and sharing of criminal intelligence information, and whether these activities have a disparate impact on minority communities, particularly Arab, Middle Eastern, Muslim and South Asian communities.

In particular, examine the fusion centers' participation in federal suspicious activity reporting, the SAR program, the Information Sharing Environment, and the FBI
eGuardian program.

The sample of SAR released in litigation or through open government requests revealed a significant number that focused on perceived race, ethnicity, national origin, and religion or other First Amendment activities, such as photography, rather than any objective facts to suggest criminal or threatening behavior.

CAIR itself was actually included in a SAR's report with a number of conspiracy theories taken off the Internet about it, so there needs to be better governance of these programs.

MR. MEDINE: Thank you very much Ms. McCaw for your comments. Any questions? Okay, thank you very much.

MR. MCCAW: Thank you.

MR. DEMPSEY: Well, again, there was a lot there. Training, it was on your list and it's on our list, the SAR was on your list and it's on our list. Would you be able to prioritize from your list one or two items?

MR. MCCAW: Sure. I mean I can do that.
We'll be entering our statement into the written record tomorrow but I can correspond and prioritize the two most important to CAIR.

MR. DEMPSEY: Okay, thank you.

MR. MEDINE: Thank you. Greg Nojeim.

MR. NOJEIM: Hi, my name is Greg Nojeim. I'm with the Center for Democracy and Technology. We're a 501(c)(3) organization in Washington, D.C., dedicated to keeping the Internet open, innovative, and free.

In the interests of full disclosure, PCLOB member Jim Dempsey is the Vice President for Policy of CDT. He did not have a hand in the preparation of the statement.

MR. DEMPSEY: Remember, I'm no longer vice president.

MR. NOJEIM: What's your title?

MR. DEMPSEY: Staff counsel, senior counsel.

MR. NOJEIM: Staff counsel, senior counsel at CDT. He didn't have a hand in the preparation of these comments or in the positions
the CDT takes on matters before the PCLOB.

I have five items that I'd like to talk about, but I'm only going to talk about two, then I'm going to pause and invite your comments and questions so we can have a discussion. If there are none, I'll get to the others. So if you want to keep your agenda no longer than you've already made it, we could have a good discussion.

So I was pleased to hear that the PCLOB is going to be looking at Executive Order 12333. This is the order that governs the surveillance and other intelligence gathering activities, including human intelligence that targets non-Americans outside the United States.

Executive Order 12333 was issued in 1981. It was modified in 2003, 2004, and most recently in 2008 to accommodate the creation of the ODNI.

As far as I know it hasn't been significantly modified to account for changes in technology or to protect privacy given those changes in technology.
It's important as part of your review to look also at the regulations that implement the executive order, in particular, DOD regulation 5240.1-R issued in 1982. It is a public document, it's available on the Internet, and it interprets provision of the executive order, and it governs Department of Defense surveillance activities that could affect U.S. persons.

It's very troubling to me, and I would think to other civil libertarians, that this public document was secretly amended by an interpretation by the Department of Justice, Ken Wainstein, to permit contact chaining, or as a legal matter to secretly permit compelled collection by the NSA of calling records and Internet transactional records of U.S. persons in the U.S., even though the public regulation prohibited that very conduct.

That's the kind of thing that we hope your review will expose and we hope it will prevent in the future going forward.

Executive Order 12333 is the basis for
bulk collection that sweeps in the communications
of many Americans, including bulk collection
disclosed in documents released by Edward
Snowden.

For example, the collection of records
of cell phone location on a mass basis, literally
millions of records every year, was revealed, as
was the direct tapping into of underseas cables
to obtain in bulk the backup of information
between servers of U.S. companies like Google and
Yahoo.

Everyone knows that the communications
going over those cables will include both
communications of U.S. persons and non-U.S.
persons, because that's who those companies
serve. Probably more non-U.S. persons than U.S.
persons.

Nonetheless, the proportion of
Americans' communications being picked up in that
surveillance is quite high. And one of the tasks
that I hope PCLOB takes on is whether the
minimization procedures that govern that bulk
collection are adequate to the task of protecting Americans' civil liberties.

Your review of Executive Order 12333 should also include an assessment of its scope. Its scope is determined by the definition of foreign intelligence information that is the basis for which collection under 12333 can be engaged in.

Foreign intelligence information is defined as information relevant to the activities and intentions of any foreign individual or organization.

That is not a meaningful limitation on this collection and we are asking that you look at that closely and assess whether it makes sense to continue to have such a broad -- how many minutes left? To have such a broad, permissive provision in the law, in the executive order.

MR. MEDINE: I'll take your bite on asking questions. Do you have suggestions about how the definition of foreign intelligence should be narrowed?
MR. NOJEIM: Yes. One possibility is to use the definition of foreign intelligence information that is in FISA. It too is quite broad, but not as broad as that.

The FISA definition of foreign intelligence includes information relevant to, let's see if I can do all of this, national security, foreign affairs, and then it's got three rather specific elements, like terrorism, and then there's two others in the front part. So that's one possibility.

But actually what I think might be a better approach would be to say that for purposes of intelligence surveillance, foreign intelligence is X, and for purposes of human or other kinds of collection foreign intelligence is Y.

When we had discussion about this with some folks in the intelligence community they pointed out that the breadth of that definition is necessary because EO 12333 governs not just intelligence surveillance but also human
intelligence. So it might be appropriate to have a bifurcated definition.

MR. DEMPSEY: Just quickly, how does that play out? Because we're targeting the intentions of a foreign leader. There are two possibilities, one is to listen to the communications to and from the foreign leader, the other is to have a human source inside the foreign leader's circle.

Why would you have different definitions of the scope of collection?

MR. NOJEIM: Because one type of surveillance -- let me put it this way --

MR. DEMPSEY: Because electronic has incidental?

MR. NOJEIM: If it's electronic, yeah.

MR. DEMPSEY: And the thing is that electronic includes incidental unavoidably.

MR. NOJEIM: Yes. Yes, well, and so might the informant in the room I guess.

But certainly the way electronic is being conducted the incidental collection is
quite high, so to offset that, one option is to limit the class of communications that can be collected in the first place.

MS. WALD: Could I ask you a another question along those lines? The FISA definition of foreign intelligence information is two tiered. One, which you've given a summary of, then it points out that if you're dealing with U.S. persons it's got a slightly higher standard, although it's unclear how that actually gets implemented, if at all, saying it's got to be necessary to, then it's security, etcetera, etcetera.

Would that two tiered approach be workable in your opinion, or what's your view on this?

MR. NOJEIM: I would ask that the Board look into what is the difference between those two, how does the government interpret related to versus necessary for?

I really don't know enough, and I don't know that there's enough in the public materials
to make an assessment. I would think that that would be the kind of thing that it would be okay to make public after looking at it really closely.

I have to say that we have, for purposes of Section 702 surveillance, advocated a narrower class of foreign intelligence information to be used for that kind of surveillance.

In particular, we said that the part of the foreign intelligence definition that governs FISA surveillance, the part that goes to mere relevance to U.S. foreign affairs should be dropped for purposes of Section 702.

An even better approach might be for using the carefully thought-out use restrictions in PPD-28 to inform the scope of permissible intelligence surveillance. I thought that aspect of PPD-28 was pretty good.

Are there more questions about 12333?

MS. BRAND: A quick question just to make sure I understand your suggestion that the definition of foreign intelligence be different
for different types of collection, I just want to make sure I understand.

Because the definition of foreign intelligence relates to what type of information you're trying to get, not so much how you get it, and if I understand what you and the colloquy that you and Jim were having, you want to limit the way in which collection is done in the electronic surveillance context because there's a higher incidence of incidental collection.

But the type of information you're trying to get is still the same, so I'm just trying to figure out how changing the definition of foreign intelligence would fix the problem that you're identifying, if that makes sense.

MR. NOJEIM: Translated into the domestic context, right, we have different investigative techniques, and we regard wiretapping, electronic surveillance as one of the most intrusive ones. For that kind of technique we require probable cause, we limit the class of people to whom that technique can be
I'm suggesting a similar concept for foreign intelligence gathering, that if it's wiretapping here, it's wiretapping there and that people abroad have rights that we need to respect.

And one of the concepts in international law is that we want to try to minimize the impact on people who have no foreign intelligence value of the collection, so you use a more restricted scope when it comes to surveillance.

MS. BRAND: I thought that's what you were getting at, and that makes sense. I think that changing the definition of foreign intelligence isn't the way to accomplish that necessarily but maybe we can talk more about it later. It's an interesting idea.

MS. WALD: Do you have also have specific, you talked about possibly looking into the need for change in the minimization rules as to some of these categories. Do you have specific proposals along those lines in writing?
MR. NOJEIM: We will. One thing that struck me though is that a lot of minimization is about masking the U.S. person's identity. And when you look at PPD-28 and how minimization, how dissemination and retention under PPD-28, the rules that govern those concepts for U.S. persons are to be applied to non-U.S. persons, one has to wonder whether, first, how that's going to be done, and secondly, whether that's adequate.

One type of minimization is to throw out information after a certain amount of time.

MS. WALD: Yes, some of us have recommended that, as you're aware.

MR. NOJEIM: And what I would have to do is look a little more deeply at how minimization is being done to see whether that retention idea is a valid one.

MR. MEDINE: Do you have a question?

MS. COLLINS COOK: I do have a question, and this is probably a question for the next speaker as well, I believe is scheduled to talk about 12333 as well.
Given that our mandate is counterterrorism, how would you suggest that we navigate what could certainly be perceived to be a tension between our statutory mandate, which is limited to counterterrorism, and for example, a review of 12333 writ large, which is obviously used for many, many purposes?

Or for example, an emphasis or a suggestion from us to change the definition of foreign intelligence, as against collection for foreign affairs purposes.

So I think, you know, we've talked a lot about this and what our mandate means and what the limits of our mandate might mean, but I'm curious to hear whether or not you've thought about the implications of our mandate for a broad review of 12333.

MR. NOJEIM: Well, you probably already crossed that rubicon in the 702 Report because the 702 surveillance is for foreign intelligence purposes, and terrorism is among them, but not the only one. So I would suggest kind of
muddling along in the same vein. I mean you're not going to say we can't look at 12333 --

MS. COLLINS COOK: I think we can do better than muddling, Greg, really, can you give us something? It's a serious question.

MR. NOJEIM: What I would suggest is that the Board discuss it and come to the conclusion that it cannot do its counterterrorism mission unless it examines intelligence gathering authorities that go beyond terrorism. It has to.

MR. MEDINE: Your time has expired, but thank you. We hope you will submit written suggestions in addition to your comments. The time has expired, thank you.

MR. NOJEIM: Thank you.

MR. MEDINE: Jeramie Scott?

MR. SCOTT: Good afternoon. My name is Jeramie Scott. I'm the National Security Counsel for the Electronic Privacy Information Center. EPIC is a public interest research institution in Washington, D.C. that was established in 1994 to focus public attention on
emerging privacy and civil liberty issues, as well as to protect constitutional values and the rule of law.

EPIC has particular interest in issues related to national security and surveillance. EPIC regularly updates and maintains multiple webpages to provide valuable information to the public about current and developing issues involving government surveillance authority and programs.

In addition, EPIC contributes to the government's understanding of these issues through amicus briefs filed in the Supreme Court and other courts across the country.

Various branches of the government, including this Board have recognized EPIC's expertise in these areas through invitations to testify in matters of government surveillance.

I would like to thank the Privacy and Civil Liberties Oversight Board for convening this public meeting today and also acknowledge the hard work of the Board over the past several
months in reviewing the use of Section 215 and 702 of the Foreign Intelligence Surveillance Act. Today though I would like to urge the Board to expand its agenda beyond Section 215 and 702, and specifically urge the Board to shift its focus to Executive Order 12333.

President Ronald Reagan signed Executive Order 12333 in September of 1981. It established broad new surveillance authorities for the intelligence community outside the scope of public law with little to no oversight in place.

In a prepared statement before the Senate Judiciary Committee, former Director of the NSA, General Keith Alexander, stated the NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by Executive Order 12333.

Through the disclosures over the past year, the American public and the rest of the world have begun to realize the extent of this surveillance conducted under 12333.

For example, under executive order
authority the NSA's MYSTIC and RETRO programs allow for the collection of a hundred percent of a foreign country's telephone calls and the subsequent retrieval of those calls at a later date.

The NSA also has tapped directly into the main communication links between Google and Yahoo data centers located around the world in order to scoop up massive amounts of data.

Additionally, it has been reported that NSA has collected hundreds of millions of contact lists from email and instant message accounts.

Undoubtedly, the NSA's mass surveillance conducted under 12333 captures huge amounts of data unrelated to the mission of national security, including information on millions of Americans.

Although 12333 requires a court order to target a United States person, this is of little comfort. Given the global nature of communications, the indiscriminate mass surveillance the NSA conducts overseas captures
the information of United States persons.

Furthermore, the government can use and share this information without any order from a judge or oversight from Congress.

As a matter of fact, the only check on surveillance under 12333 comes from executive oversight. This type of self-regulation has proven to be ineffective at best in limiting surveillance overreach.

The minimal oversight in place does not even give the appearance of the checks and balances provided by judicial or congressional oversight. Congress has admitted to very little oversight of the activities under 12333.

Additionally, Executive Order 12333 does not fall within the purview of the Foreign Intelligence Surveillance Court, thus no neutral arbiter reviews 12333 surveillance for compliance with the Fourth Amendment.

As the Chief Justice recently explained, the Fourth Amendment was the founding generation's response to the reviled general
warrants and writs of assistance of the colonial era, which allowed British officers to rummage through homes in an unrestrained search of evidence of criminal activity.

It is clear that the surveillance programs and activities under Executive Order 12333 require further scrutiny and these activities fall squarely within the Board's jurisdiction.

I urge the Board to review 12333 and recommend the Board oversee, one, the extent to which information on United States persons is captured by surveillance conducted under 12333. Two, the extent to which collection under 12333 results in the retention and/or dissemination of non-target data. Three, the effectiveness of current oversight and minimization procedures.

Furthermore, EPIC recommends a public report of the Board's findings.

Thank you for the opportunity to appear before the Board today.
MR. MEDINE: Thank you, Mr. Scott. Any questions? Thank you very much.

The final speaker today will be John Tye.

MR. TYE: Hello, my name is John Tye. I used to work at the U.S. Department of State in the Bureau of Democracy, Human Rights, and Labor. I worked there from 2011 through April of this year.

Now I work at an NGO called Avaaz, which is a global civic organization with over thirty-seven million members around the world.

While I was at the Department of State actually my job was to work on Internet freedom policies, so both freedom of expression, freedom of assembly, association, but also privacy rights. And while I was there, I had a clearance to receive top secret information and sensitive compartmented information, TS/SCI.

Part of my work in that capacity was, included, you know, diplomatic efforts related to the scope of privacy rights included in U.S.
treaty obligations, so the International Covenant on Civil and Political Rights, for example. And there were various resolutions at the U.N. General Assembly, at the U.N. Human Rights Council. That's sort of how I got to learn some of the things I came to talk about today.

And really the reason I'm here today is to talk about an untold story of constitutional violations under Executive Order 12333.

And I actually wrote about this in the Washington Post. It was published on Sunday and some of you may have seen that.

Even after all of the disclosures of the past year and all of the reforms announced by the President in January, the American people still haven't heard about the NSA activities that are most intrusive to their privacy.

And in my view, based partly on classified facts, Americans should be far more concerned with the collection and storage of their communications under 12333 than under the PATRIOT Act or the Foreign Intelligence
Surveillance Act.

12333 is a legal loophole that allows the NSA to collect a huge amount of domestic U.S. communications to Americans, from Americans, by Americans just so long as those communications are collected outside the borders of the United States.

Because of the structure of the global Internet, a very large portion of Americans' communications are available for collection outside of our borders.

For example, we're here in Washington, D.C. and we're just a couple of blocks from the White House. Let's say hypothetically I was using Gmail, or Yahoo, or another big email provider, and sitting right here I sent an email to the President at that White House just two blocks away, it's almost certain that that email would be stored on servers around the world. So a lot of these server networks have mirror servers in countries like Brazil, Japan, South Korea, the United Kingdom, all over the world.
So there's nothing in Executive Order 12333 that would prevent the NSA from collecting that email from here, two blocks away, and all such emails between U.S. persons in the United States.

And the same thing is true for almost every communication that Americans make, whether it's an email, an instant message, a Skype conversation, or even many phone calls.

12333 doesn't limit the volume of U.S. person communications that can be collected under its authority, and the Director of National Intelligence has recently declassified a document showing that the NSA is authorized to retain Americans' communications for up to five years when they're collected under 12333.

So in part based on classified facts that obviously I couldn't discuss in this setting, but that I lawfully had access to while I was employed at the Department of State, I filed a complaint with the Inspectors General at both the Department of State and the National
Security Agency, and met with staffers in both the House and Senate Intelligence Committees in Congress.

One of the issues that's been noted by previous speakers is there's basically no meaningful oversight outside of the executive branch of activities conducted under 12333.

In the USA FREEDOM Act, which of course was passed by the House and is being debated in the Senate, which some people hope will help to address problematic NSA activities, would actually do nothing to address this very large legal loophole.

And so in my view, while the public debate over the last year has focused largely, at least with respect to U.S. person communications, has focused largely on Section 215 and 702, 12333 is a much greater concern.

I hope that the President would revise this executive order immediately to require the NSA to purge U.S. person communications or data as soon as it's incidentally collected so that it
can't be stored, it can't be queried.

That's actually the same thing, you all are of course very familiar with the Review Group on Intelligence and Communication Technologies.

In recommendation 12 of their report they actually said the same thing, that incidentally collected communications under 12333 should be immediately deleted. There's been no public comment from the administration on that recommendation.

I'd also suggest that Congress should pass legislation setting minimum privacy standards for U.S. persons across all of the different intelligence authorities.

The last thing I'd like to say is, you know, it's a little bit scary coming up here talking in public about these issues. And you know, it's true, I mean if I did say the wrong thing I could go to prison, and it's a serious thing, so you know, I've retained a lawyer and other things just to make sure I'm following the rules because I want to make sure I do that.
I will say, you know, for over a year the President has been saying that whistleblowers have legal options to raise their concerns without illegally disclosing classified information and I see my complaint as a chance for the President to show that he means what he says when he said that.

I haven't broken any laws. I haven't disclosed classified information improperly. I had my op-ed cleared by both the NSA and the State Department in pre-publication review to ensure that it contained no classified materials.

I guess the last thing before I take questions would be if you all would like to meet in a classified setting we could probably arrange a way to do that and go into more detail. Thanks.

(Applause)

MR. MEDINE: Thank you. Any questions? MS. COLLINS COOK: I did have a question actually, and it builds on something that we've thought about, talked about and appeared in some
part in our 702 Report, particularly the separate statements.

Your suggestion that all U.S. person communications that are incidentally collected be purged at collection, how would that work, that's my question?

So, for example, would analysts be required to review every communication, even communications they wouldn't otherwise review to determine whether or not these were U.S. person communications and then purge them?

Would they have to do additional investigation to determine they are U.S. person communications?

I'm just curious as to, it is a suggestion we've heard. It's something we've considered. I find myself, I find it very hard to get past some of these threshold questions and whether it is more privacy protective, for example, to require review of communications that would not otherwise be reviewed in order to determine whether or not they should then be
MR. TYE: It's a good question. I think it depends some on the technical mechanism that this is carried out with. And the truth is I don't know all the details of those mechanisms. I could speculate but I don't think I could give you a helpful answer on that question.

MS. COLLINS COOK: Perhaps if you do choose to do a written submission you could expound a little bit on what you meant by your recommendation that U.S. person communications be purged at collection. I think it's a very, very difficult question and I am interested in your views as to how that might be implemented.

MR. TYE: Okay, thank you.

MS. WALD: If it's of any assistance to you in responding to my colleague's request, you might look at our separate statement in which we looked at that, the Chairman and mine, the specific question.

The usual justification for not doing anything at all in reviewing was, well, somebody
can't tell that something that looks innocent
today might a year from now, or two years from
now somehow be part of a more intricate mosaic
and so therefore, you know, just forget about it.

I assume there could be a rule or we
suggested several outs on that, but there could
be a rule of reason. These analysts make
judgments all the time about what is intelligence
information and what is not. That's their job
and I'm sure that they're good at it.

And so the question about whether you
can make a reasonable decision about whether
something has foreign intelligence view, even if
you can't predict that there's a hundred percent
chance that in five years something might come up
that would make it more relevant, still you've
got to weigh the privacy implications against the
dangers that you have suggested in your op-ed
page in the Washington Post.

MS. COLLINS COOK: Could I make sure I
understand? Perhaps I misheard your
recommendation. I thought your recommendation
1 did not turn on whether or not there was foreign
2 intelligence information within the
3 communications. It was simply that to the extent
4 these are incidentally collected U.S. person
5 communications they should be purged, regardless
6 of potential value.
7          MR. TYE: Yeah.
8          MS. COLLINS COOK: That's your
9 recommendation?
10          MR. TYE: Yeah, so my recommendation is
11 the exact same one that the review group made in
12 recommendation 12.
13          MR. DEMPSEY: A quick question, you
14 filed a complaint with the State Department IG,
15 right?
16          MR. TYE: Yes, correct.
17          MR. DEMPSEY: And with NSA also.
18          MR. TYE: Well, so I first met with the
19 State Department Inspector General, then I met
20 with the two staffers from both of the
21 intelligence committees, then I left federal
22 employment and about maybe, I would have to go
back and look at the dates, but about a couple of weeks later I was invited to meet with the NSA.

MR. DEMPSEY: And the complaint, was that written?

MR. TYE: No, it was not in writing because I didn't have access to a classified system, computer system.

MR. DEMPSEY: You mean the one you did when you were in government? So in other words, if we asked to see a copy of the --

MR. TYE: There are presumably notes.

MR. DEMPSEY: Right, but not a paper submission?

MR. TYE: I did not make a paper submission, no.

MR. DEMPSEY: Okay, okay.

MS. BRAND: I don't have a question, but I just want to make a quick comment. It seems that you've taken great care in following the applicable rules and procedures and laws in pursuing your complaint, so without making any statement about whether I agree with you, I
applaud you for taking care and following the rules. That's commendable.

MR. TYE: Thank you.

MR. MEDINE: And I also applaud you for being here today and being willing to speak publicly about these issues, and we appreciate that.

Thank you for your comments and suggestions, and thanks to all the speakers for their very constructive and thoughtful comments. And again, we would invite the speakers and any others who have thoughts about our future agenda to submit written comments through regulations.gov where we will keep the record open through the end of August.

If there are no other matters, the Board's activities for today are now complete. A transcript of today's meeting will be available on our website, pclob.gov. All in favor of adjourning the meeting say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous
consent to adjourn, we are now adjourned. It is 2:20 p.m. Thank you.

(Whereupon, at 2:20 p.m., the meeting was adjourned.)
CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of the State of Maryland, Baltimore County, do hereby certify that the proceedings contained herein were recorded by me stenographically; that this transcript is a true record of the proceedings.

I further certify that I am not of counsel to any of the parties, nor in any way interested in the outcome of this action.

As witness my hand and notarial seal this _______ day of ______________________________, 2014.

______________________________
Lynne Livingston
Notary Public

My commission expires: December 10, 2014
improperly 43:10 71:9
improve 12:18
inability 19:1
inaccurate 43:17 44:5
inappropriate 34:14
inappropriately 37:10
incidence 55:10
incidental 52:15 52:18,22 55:10
incidentally 69:22 70:7 72:4 75:4
include 37:15 49:13 50:4
included 17:8 45:9 65:21,22
includes 51:6 52:18
inclusion 36:9
income 23:20
incorrect 43:14
increase 4:19
independence 21:19,22
independent 19:20 24:11 25:16 30:3
indiscriminate 62:21
individual 18:9 18:16 50:11
individuals 35:7 36:17,21 40:16 41:11 43:18
ineffective 63:8
infiltrate 40:12
infiltrated 18:17
infiltrating 18:13
infiltration 16:12 18:10 21:13
inform 54:16
informant 17:9 40:22 52:20
informant led 40:19
informants 35:9 40:12 41:9
informative 12:9
informs 14:18
infrastructure 18:22
initiate 28:15 38:2
initiated 23:15
initiative 10:14 20:12,15
innocent 74:1
innovative 46:10
input 3:22 8:22
inside 52:8
insight 22:19
insisting 38:15
inspector 75:19
inspectors 28:10 68:21
instance 15:13 23:10,12,22
instances 15:15
instant 62:12 68:8
institution 22:22 59:21
institutional 15:16 17:5 23:11
instructions 44:5
instructors 43:16
integrity 25:18
interconnected
35:18
interest 59:20 60:4
interested 73:13 79:12
interesting 17:5 56:17
interests 46:11 interlaces 18:15
internal 12:4 26:10
international 56:7 66:1
interpret 53:19
interpretation 22:2 48:12
interprets 48:6
interviews 35:3
intricate
intrusive 38:3 55:20 66:17
inventory 7:8
investigate 15:3 41:13
investigating 14:1
investigation 22:9 72:13
investigative 38:3 55:18
invitations 60:17
invite 47:4 77:11
invited 13:10
involve 7:20
involvement 43:7
involving 18:13 19:12 60:9
involves 26:15 56:15
isolated 15:13
issue 17:14 18:4 28:4 30:12
issued 4:15 7:18 47:15
item 3:17 5:15
items 45:21 47:2
ive 13:15 70:20

J
james 2:5 22:18
january 6:6 66:15
japan 67:21
jeramie 2:17 59:16,18
jim 46:12 55:7
job 65:14 74:9
john 2:19 23:5 65:3,5
joined 9:14 38:13
jones 40:20
journey 28:4
judge 35:11 63:4
judgments 74:8
Public Meeting

July 23, 2014

Henderson Legal Services, Inc.

202-220-4158  www.hendersonlegalservices.com
Public Meeting
July 23, 2014

Henderson Legal Services, Inc.
202-220-4158 www.hendersonlegalservices.com
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>47:16</td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td>47:16</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>19:12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>47:17</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>19:12</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>17:13</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>42:10 65:8</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>4:7</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>1:9 3:5,8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4:7 79:15,20</td>
<td></td>
</tr>
<tr>
<td>215</td>
<td>4:13 6:4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>22:1 61:1,4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>69:17</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>1:9 3:5</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>6:7</td>
<td></td>
</tr>
<tr>
<td>2nd</td>
<td>4:15</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9th</td>
<td>3:8</td>
<td></td>
</tr>
</tbody>
</table>