BRENNAN
CENTER
FOR JUSTICE

Brennan Center for Justice
at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
646.292.8310 Fax 212.463.7308
www.brennancenter.org

MEMORANDUM

To: Privacy and Civil Liberties Oversight Board

From: The Brennan Center for Justice

Re: Agenda of the Privacy and Civil Liberties Oversight Board

Date: October 26, 2012

The Brennan Center for Justice welcomes the opportunity to submit written comments to the Privacy and Civil Liberties Oversight Board (PCLOB) regarding the Board's agenda, pursuant to the notice published in the Federal Register on October 23, 2012, at 77 FR 64835.

There are a number of issues that will warrant the PCLOB's attention. The Brennan Center wishes to draw attention to some of the most pressing civil liberties issues within the three main areas on which our own current work is focused: (1) religious profiling; (2) information privacy; and (3) transparency. We would be happy to provide additional information on any of these matters and look forward to working closely with the PCLOB as it establishes its agenda and begins to focus on specific tasks.

Religious profiling

1) Impact of Unproven Radicalization Theory

Many agencies in the federal government have embraced a theory about how American Muslims become radicalized to violence. These theories assume that there is a sort of "religious conveyor belt" that leads directly from embracing a conservative strain

of Islam to terrorism.[1] But the religious conveyor belt theory is simply not supported by evidence. Decades of research by governments and social scientists demonstrate that there is no single path to terrorism and no single profile of a terrorist.

Unthinking acceptance of the flawed religious conveyor belt theory, particularly by law enforcement agencies such as the FBI, has enormous negative consequences. It undergirds the view that our national security is served by monitoring the religious views of American Muslims to identify potential terrorists. The result has been widespread surveillance of Muslim communities that is unconnected to any suspicion of criminal or terrorist activity. We urge the PCLOB to consider the full range of issues relating to radicalization, including the very real impact of the religious conveyor belt theory on the First Amendment rights of American Muslims.

2) 2003 DOJ Racial Profiling Guidance

In June 2003, the Department of Justice issued Guidance Regarding the Use of Race by Federal Law Enforcement Agencies.[2] That guidance does not prohibit profiling on the basis of religion or national origin. Moreover, the guidance gives law enforcement officers wider latitude to consider race and ethnicity in matters involving national security and border integrity.[3] Evidence is accumulating that law enforcement agencies are engaged in religious profiling in their counterterrorism efforts.[4]

---

[1] For a detailed discussion of radicalization theories, *see* FAIZA PATEL, BRENNAN CENTER FOR JUSTICE, RETHINKING RADICALIZATION (2011), *available at* http://brennan.3cdn.net/f737600b433d98d25e_6pm6beukt.pdf. *See also The American Muslim Response to Hearings on Radicalization Within Their Community, Hearing Before the H. Comm. on Homeland Sec.*, 112th Cong. (2012) (written submission of Faiza Patel, Co-Director, Liberty and National Security Program, Brennan Center for Justice at NYU School of Law), *available at* http://www.brennancenter.org/content/resource/testimony_for_hearing_on_the_american_muslim_response_to_hearings_on_radica/.

[2] *See* U.S. DEPT. OF JUSTICE, GUIDANCE REGARDING THE USE OF RACE BY FEDERAL LAW ENFORCEMENT AGENCIES (2003), *available at* http://www.justice.gov/crt/about/spl/documents/guidance_on_race.pdf.

[3] *Id.* at 9.

[4] *See Ending Racial Profiling in America, Hearing Before the Subcomm. on the Constitution, Civil Rights,*

In addition to violating individuals' civil liberties, profiling on the grounds of race, ethnicity, religion, or national origin is simply an ineffective method of law enforcement. It is thus particularly perverse to engage in such profiling in national security or border integrity cases, where the stakes are highest and *behavioral* profiling is the gold standard.[5] Indeed, Senators Richard Durbin and John Conyers have urged Attorney General Holder to revise the Guidance to close the loopholes in the Justice Department's guidance,[6] and the American Bar Association recently amended its own racial profiling statement to urge law enforcement agencies to ban religious profiling.[7] We encourage the PCLOB to similarly recommend that the Attorney General revise the guidance.

3) 2008 Attorney General's Guidelines for Domestic FBI Operations

The Attorney General's Guidelines for Domestic FBI Operations govern the opening and management of all FBI matters.[8] In recent years, the Guidelines were

---

and Human Rights of the S. Comm. on the Judiciary, 112th Cong. (2012) (written statement for the record submitted by Faiza Patel and Elizabeth Goitein), *available at* http://www.brennancenter.org/content/resource/testimony_for_hearing_on_ending_racial_profiling_in_america/

[5] *See, e.g.*, RIGHTS WORKING GROUP, RACIAL PROFILING: UNJUST, INEFFECTIVE, AND COUNTERPRODUCTIVE (2011), *available at* http://www.rightsworkinggroup.org/sites/default/files/RacialProfiling_IssueBrief.pdf.

[6] *See* Dear Colleague Letter, Sen. Richard J. Durbin and Sen. John Conyers, Jr. (March 19, 2012), *available at* http://durbin.senate.gov/public/index.cfm/files/serve?File_id=7baef783-49a0-47f9-a71b-1b18797fb542.

[7] *See* American Bar Association, House of Delegates Resolution 116, adopted Aug. 7, 2012, *available at* http://www.abanow.org/2012/06/2012am116/.

[8] The version of the Guidelines currently in use was issued by Attorney General Mukasey. *See* MICHAEL B. MUKASEY, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS [hereinafter "Mukasey Guidelines"], *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf. The AG Guidelines are supplemented by the FBI's Domestic Investigations and Operations Guide and a Baseline Collection Plan. The Domestic Investigations and Operations Guide, or DIOG, last revised in 2011, is available at http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version, and the Baseline Collection Plan, issued in November 2009, is available at http://www.aclu.org/files/fbimappingfoia/20111019/ACLURM004887.pdf. For a detailed analysis of the evolution of the Attorney General's Guidelines, including the expansion of the FBI's surveillance authorities and the increased risk of infringements upon individuals' privacy and civil liberties, *see* EMILY BERMAN, BRENNAN CENTER FOR JUSTICE, DOMESTIC INTELLIGENCE: NEW POWERS, NEW RISKS (2011),

watered down in two ways that have significant implications for civil liberties. We would ask the PCLOB to engage in a careful review these two changes and their impact.

First, under Attorney General Ashcroft, the Guidelines were amended to eliminate the requirement that reasonable suspicion of criminal activity be present before monitoring First Amendment-protected activities and organizations.[9] It is now permissible for agents and informants to attend religious or political gatherings without any basis for suspecting wrongdoing. In 2010, the Justice Department's Inspector General issued a report finding that the FBI had engaged in numerous questionable uses of this authority.[10] The report underscores the potential for First Amendment activities to be chilled in exactly the manner the "reasonable suspicion" requirement was intended to prevent.

Second, under the 2008 guidelines issued by Attorney General Mukasey, a new category of "assessments" was created in which agents are permitted to use certain techniques (including 24-hour physical surveillance, the use of informants, and the use of "pretext interviews") that were previously reserved for predicated investigations – i.e., investigations in which there is some factual predicate to suspect wrongdoing.[11] The requirement of a factual predicate was a key bulwark against racial, ethnic, religious, and political profiling. Indeed, the Domestic Investigative Operational Guidelines (DIOG), which implement the Attorney General's Guidelines, allow agents to open assessments on the basis of First Amendment-protected activity or a target's race, religion, or national

---

available at http://brennan.3cdn.net/9372cfab2b4be86fd8_41m6b858n.pdf.

[9] JOHN ASHCROFT, U.S. DEPT' OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS § VI.A. & B (2002), *available at* http://www.fas.org/irp/agency/doj/fbi/generalcrimes2.pdf.

[10] U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FBI'S INVESTIGATION OF CERTAIN DOMESTIC ADVOCACY GROUPS 188 (2010).

[11] Mukasey Guidelines, *supra* note 8, § II.

origin, as long as those are not the *only* justifications.[12] The change thus opens the door to such profiling, as well as to undue intrusions on all Americans' privacy.

Information Privacy

1) Third-party records

Since 9/11, the federal government has sought to amass private information about U.S. persons though the collection of "third party records" held by cell phone providers, internet service providers, and web-based companies such as Google, Facebook, and Twitter. Such records may include the contents of email communications, online browsing activity, and geolocation data generated by cell phones. The government invokes a patchwork of different authorities to obtain access to this information without probable cause, including Section 2703 of the Electronic Communications Privacy Act and Section 215 of the Patriot Act. The government has also adopted broad and sometimes secret interpretations of its authority under these laws, in an apparent end run around the Fourth Amendment.[13] We therefore ask the PLCOB to examine the various circumstances under which the government may obtain access to third party records and assess whether existing laws are sufficient to protect the privacy of electronic communications and sensitive geolocation data.

2) National Security Agency collection

Several former National Security Agency employees have described an extensive domestic surveillance program that is gathering the personal communications of millions of Americans who are not suspected of a crime. According to these employees, the NSA has installed listening posts within private telecommunications companies and is

[12] U.S. DEP'T OF JUSTICE, FBI, DOMESTIC INVESTIGATIVE OPERATIONAL GUIDELINES, §§ 3, 5.1.
[13] *See generally*, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, ELECTRONIC SURVEILLANCE & GOVERNMENT ACCESS TO THIRD PARTY RECORDS (2012), *available at* http://www.nacdl.org/reports/thirdpartyrecords/thirdpartyrecords_pdf/.

collecting and storing a vast array of electronic communications for future searching and analysis.[14] In addition, the NSA recently acknowledged that its spying activities have, on at least one occasion, violated the Fourth Amendment to the Constitution.[15] The NSA's program of intelligence collection and retention is sorely in need of oversight and reform.

3) Searches of electronic devices at the border

Under the border search exception to the Fourth Amendment, which was originally developed to cover searches of physical items like the contents of a suitcase, the government in recent years has asserted (and courts have generally confirmed) the right to search the contents of travelers' electronic devices – including phones, computers, and cameras – with no suspicion of wrongdoing. In addition, the government can retain the documents, pictures, electronic messages, and other materials it finds for a certain period of time for analysis and technical assistance, and can share those materials with other agencies.[16] This is a dramatic change from previous policy: as recently as 2000, published customs directives prohibited agents from reading personal documents carried by travelers unless agents had "reasonable suspicion" to suspect that the documents constituted contraband.[17]

---

[14] *See, e.g.*, James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED, March 15, 2012, *available at* http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/; Shane Harris, *Giving in to the Surveillance State*, N.Y. TIMES, Aug. 22, 2012, *available at* http://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html.

[15] *See* Siobhan Gorman, *Spy Agency Activities Violated Fourth Amendment Rights, Letter Discloses*, WALL STREET JOURNAL, July 20, 2012, *available at* http://online.wsj.com/article/SB10000872396390444097904577539413137490028.html.

[16] *See* U.S. DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE BORDER SEARCHES OF ELECTRONIC DEVICES (2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf.

[17] *Compare* U.S. CUSTOMS & BORDER PROTECTION, CUSTOMS DIRECTIVE 3340-006A, PROCEDURES FOR EXAMINING DOCUMENTS AND PAPERS, §§ 6.4, 6.5 (2000) (permitting officers to "glance" at documents to see if they are merchandise, but requiring reasonable suspicion to read documents), *available at* http://www.aclu.org/files/pdfs/natsec/laptopsearch/dhs_20100816_DHS000742-DHS000745.pdf, *with* U.S. CUSTOMS & BORDER PROTECTION, POLICY REGARDING BORDER SEARCH OF INFORMATION 1 (2008) (permitting officers to "read and analyze" a traveler's documents without reasonable suspicion), *available at* http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf.

In an age when computing power, memory, and storage enables travelers to carry, in effect, their whole lives with them when they travel, the government's new policy allows it to engage in breathtakingly intrusive searches that would otherwise require a warrant, solely because the target of the search happens to be at a U.S. border. The PCLOB should review the government's position and published guidance on this matter and recommend modifications to better safeguard travelers' reasonable expectations of privacy.

4) Drone surveillance

The development of drone technology is occurring at breakneck speed, and nearly every day brings reports of new types of drones launched in civilian airspace. While the FAA has been statutorily required to develop a safety plan for "civil unmanned aircraft systems,"[18] and the Air Force has released a directive governing the sharing and retention of information collected about U.S. persons,[19] no federal agency has been tasked with developing privacy guidelines for civilian drones. The PCLOB should examine the privacy risks posed by civilian drones, identify the appropriate governmental body to craft binding privacy and civil liberties protections, and provide detailed recommendations for what those protections should entail.

5) NCTC Guidelines

In March 2012, the Office of the Director of National Intelligence released new guidelines for the National Counterterrorism Center.[20] Those guidelines make a number

[18] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332 (2012).
[19] DEP'T OF THE AIR FORCE, AIR FORCE INSTRUCTION 14-104, OVERSIGHT OF INTELLIGENCE ACTIVITIES (2012), *available at* http://www.fas.org/irp/doddir/usaf/afi14-104.pdf.
[20] *See* NAT'L COUNTERTERRORISM CTR., GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION (2012), *available at* http://www.fas.org/sgp/othergov/intel/nctc_guidelines.pdf.

of changes to the previous guidelines, issued in 2008; the most critical revision is that the NCTC is now empowered to query, access, and, in some cases, copy entire federal databases of information relating to U.S. persons as long as there is *some* "terrorism information" in the database. The NCTC has not publicly explained why it needs this sweeping new authority, which would appear to apply to nearly any federal database, including databases that were collected for reasons far afield from counterterrorism. Moreover, the guidelines themselves specifically contemplate that the PCLOB will conduct oversight over the operations of the NCTC, including its compliance with constitutional limitations. The PCLOB should begin exercising that oversight immediately, and should inspect whether the NCTC's new authority has been appropriately balanced against protections for privacy and civil liberties.

Transparency

1) Classification Reform

The classification of information that poses no real threat to national security has been a problem for decades. Experts estimate that between 50-90% of classified documents could safely be released.[21] This near-habitual "overclassification" raises enormous problems for civil liberties oversight and accountability. While the Public Interest Declassification Board (PIDB) has been charged with developing recommendations to reform the classification system, we believe it is important for the PCLOB to weigh in on these recommendations – and perhaps provide its own – to ensure reforms that provide sufficient transparency to allow meaningful oversight of

[21] *See Emerging Threats: Overclassification and Pseudo-Classification: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, and Int'l Relations of the H. Comm. on Gov't Reform*, 109th Cong. 115 (2005) (written statement of Thomas Blanton, Director, National Security Archive).

counterterrorism policies by executive oversight bodies, the co-equal branches of government, and the public.

2) Secret Law

The Executive branch and, increasingly, the courts are developing a body of "secret law" that inhibits public discussion and debate regarding our nation's counterterrorism policies.[22] Manifestations of "secret law" include secret opinions of the Justice Department's Office of Legal Counsel, classified executive orders and other presidential directives, classified opinions of the Foreign Intelligence Surveillance Court, and the growing practice of sealing filings, closing hearings, and redacting opinions in judicial proceedings involving questions of national security. Because of this secrecy, the public today does not know what law governs the targeted killings of U.S. citizens,[23] the permissible uses of Section 215 of the Patriot Act (which Senators Ron Wyden and Mark Udall have asserted is being interpreted in a way that will leave the American public "stunned" and "angry"[24]), or under what circumstances and individual may be detained as an "enemy combatant." The PCLOB should investigate whether this secret law in fact comports with constitutional requirements and press for additional disclosure to the maximum extent possible.

3) Secrecy in the Courts

The PCLOB should closely examine two policies that currently threaten to transform the courts' role from that of vindicating civil liberties violations to that of

---

[22] *See generally, Secret Law and the Threat to Democratic and Accountable Government: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. (2008).
[23] *See* Joe Coscarelli, *New York Times Suing Justice Department Over Targeted Killing Memo*, NEW YORK, Dec. 23, 2011, *available at* http://nymag.com/daily/intel/2011/12/new-york-times-suing-over-targeted-killing-memo.html.
[24] *See* Charlie Savage, *Senators Say Patriot Act Is Being Misinterpreted*, N.Y. TIMES, May 26, 2011, *available at* http://www.nytimes.com/2011/05/27/us/27patriot.html.

enabling them. The first is the Justice Department's 2009 policy on the use of the state secrets privilege in civil litigation.[25] While the policy provides some welcome procedural protections against abuse, it nonetheless permits the Justice Department to continue the post-9/11 trend of using the privilege as a jurisdictional bar rather than an evidentiary privilege, and the Department has frequently used the privilege in this manner. There is no national security-related reason why a claim of privilege should terminate a case at the pleadings stage, rather than allowing discovery to take place and having the court examine *in camera* any responsive evidence that the government identifies to the court as being privileged.

Second, the current Justice Department has brought more criminal prosecutions for alleged leaks of classified information to the media than all previous administrations combined. Several of these prosecutions have targeted national security whistleblowers who exposed government fraud, waste, or abuse, including torture and illegal surveillance.[26] This whistleblower prosecution policy not only threatens the civil liberties of the whistleblowers; it also discourages national security officials from bringing to light violations of the civil liberties of all Americans.

* * * * *

[25] Attorney General Eric Holder, Memorandum for Heads of Executive Departments and Agencies on Policies and Procedures Governing the Invocation of the State Secrets Privilege (Sept. 23, 2009), *available at* http://www.justice.gov/opa/documents/state-secret-privileges.pdf.

[26] *See* Phil Mattingly and Hans Nichols, *Obama Pursuing Leakers Sends Warning to Whistle-Blowers*, BLOOMBERG, Oct. 17, 2012, *available at* http://www.bloomberg.com/news/2012-10-18/obama-pursuing-leakers-sends-warning-to-whistle-blowers.html.