Description of document:	Privacy and Civil Liberties Oversight Board (PCLOB) New Hire Recommended Readings, 2017
Requested date:	06-October-2017
Release date:	09-November-2017
Posted date:	14-January-2019
Source of document:	FOIA Request Privacy and Civil Liberties Oversight Board 800 N Capitol St. NW Washington DC 20002 Fax: (202) 296-4395 Email: foia@pclob.gov

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
WASHINGTON, D.C. 20511

November 9, 2017

Re: PCLOB FOIA 2017-041

This letter responds to your Freedom of Information Act ("FOIA") request dated October 6, 2017 and received by PCLOB on October 18, 2017, in which you seek a copy of the "listing of New Hire Recommended Reading on the internal O drive at O:\Library – New Hire." The requested listing is attached.

You may contact me or the PCLOB's FOIA Public Liaison Eric Broxmeyer at (202) 331-1986 or foia@pclob.gov for further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services ("OGIS") at the National Archives and Records Administration ("NARA") to inquire about the FOIA mediation services they offer. The contact information for OGIS is Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; email at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you are not satisfied with my response to this request, you may administratively appeal by writing to the PCLOB Freedom of Information Act Appeal Authority, at MS2 Room 2C104, Washington, DC 20511, or you may submit an appeal via email to foia@pclob.gov. Your appeal must be postmarked or electronically transmitted within ninety calendar days from the date of this letter.

Sincerely,

Annan Mortensen
Acting Freedom of Information Act Officer
Attorney-Advisor
(202) 296-2706

PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

New Hire Recommended Readings

The Privacy and Civil Liberties Oversight Board is an independent, bipartisan agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007 ("9/11 Commission Act"). The Board's mission is to ensure that the executive branch's efforts to protect the nation from terrorism are balanced with the need to protect privacy and civil liberties.

The following is a list of counterterrorism and privacy/civil liberties related reports, intended for use by PCLOB new hires.

- **Office of the Director of National Intelligence: *"The Principles of Intelligence Transparency for the Intelligence Community"* https://fas.org/irp/eprint/ic-trans.pdf**
  The Principles of Intelligence Transparency for the Intelligence Community ("IC") facilitate IC decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security.

- **Adam Klein, Michèle Flournoy, and Richard Fontaine: Center for a New American Security: "*Surveillance Policy: A Pragmatic Agenda for 2017 And Beyond*" https://www.cnas.org/events/surveillance-policy-a-pragmatic-agenda-for-2017-and-beyond**
  This policy provides information on the key issues in surveillance policy facing the incoming administration and Congress. Questions discussed include: How should the new administration approach the reauthorization of Section 702? Should the new administration press for decryption legislation or seek to de-escalate the encryption controversy? How can the new administration address enduring transatlantic fissures over surveillance policy, particularly in light of pending judicial challenges to the new Privacy Shield agreement? How can surveillance decisions better account for outside equities, including cybersecurity and the technology industry's international competitiveness?

- **The National Academies Press: "*Protecting Individual Privacy in the Struggle against Terrorists: A Framework for Program Assessment*" https://doi.org/10.17226/12452**
  All U.S. agencies with counterterrorism programs that collect or "mine" personal data—such as phone records or Web sites visited—should evaluate the programs' effectiveness, lawfulness, and impact on privacy. Agencies can use a framework to evaluate such information-based programs, both classified and unclassified. The book urges Congress to re-examine existing privacy law to assess how to protect privacy in current and future programs and recommends that any individuals harmed by violations of privacy receive a meaningful form of redress.

- **Rachel Levinson-Waldman: Brennan Center for Justice at New York University School of Law: "*What the Government Does With Americans' Data*" https://www.brennancenter.org/publication/what-government-does-americans-data**
  The Brennan Center takes a comprehensive look at the multiple ways U.S. intelligence agencies collect, share, and store data on average Americans. The report, which surveys five intelligence agencies, finds that non-terrorism related data can be kept for up to 75 years or more, clogging national security databases and creating opportunities for abuse, and recommends multiple reforms that seek to tighten control over the government's handling of Americans' information.

- **Nick Adams, Ted Nordhaus and Michael Shellenberger: Breakthrough Institute: "*Counterterrorism Since 9/11: Evaluating the Efficacy of Controversial Tactics*" https://thebreakthrough.org/images/pdfs/CCT_Report_revised-3-31-11a.pdf**
  In the wake of 9/11, the U.S. government employed several new counterterrorism tactics. The tactics included interrogation, preventative detention, expanded use of secret surveillance without warrants, ethnic/religious profiling, the collection and mining of domestic data, and the prosecution of terror suspects in military tribunals. While there has been great debate over these measures, there has been significantly less attention dedicated to evaluating whether the tactics work to prevent terrorism. Even so, people on both sides of the security v. morality/legality debate make assumptions about the efficacy of various counterterrorism measures.

- **Business Executives for National Security: "*Domestic Security: Confronting a Changing Threat to Ensure Public Safety and Civil Liberties*" https://www.bens.org/file/CounterterrorismReport.pdf**
  This report assesses whether the many reforms enacted after the September 11, 2001 terror attacks are still effective at confronting a changing terrorist threat. This report also addresses the lack of an enterprise-wide concept at the federal level for U.S. law enforcement and intelligence agencies operations.

- **Gina Marie Stevens and Charles Doyle: Congressional Research Service: "*Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*" https://digital.library.unt.edu/ark:/67531/metacrs10538/m1/1/high_res_d/98-326_2008Sep02.pdf**
  This report provides an overview of federal law governing wiretapping and electronic eavesdropping. It also appends citations to state law in the area and contains a bibliography of legal commentary as well as the text of the Electronic Communications Privacy Act ("ECPA") and the Foreign Intelligence Surveillance Act ("FISA").

- **Richard M. Thompson II: Congressional Research Service: "*The Fourth Amendment Third-Party Doctrine*" https://fas.org/sgp/crs/misc/R43586.pdf**
  This report explores the third-party doctrine, including its historical background, its legal and practical foundations, and its present and future applications. The report includes arguments that support, as well as criticize the third-party doctrine.

- **Jane Chong: Lawfare: "*E.O. 12333 Raw SIGINT Availability Procedure: A Quick and Dirty Summary*" https://lawfareblog.com/eo-12333-raw-sigint-availability-procedures-quick-and-dirty-summary**

This is a description of the 10 actions outlining the procedures IC elements must follow when requesting, protecting, processing, retaining, disseminating, overseeing, and utilizing raw SIGINT. Raw SIGINT is "signals intelligence and associated data that has not been evaluated for foreign intelligence purposes and/or minimized."

- **The Constitution Project's Liberty and Security Committee: *"The Case for a FISA "Special Advocate"* http://www.constitutionproject.org/wp-content/uploads/2014/05/The-Case-for-a-FISA-Special-Advocate_FINAL.pdf**
  Edward Snowden's disclosures prompted a public debate over the proper scope of the government's surveillance authorities—and the efficacy of the largely secret oversight and accountability mechanisms Congress has designed to oversee them. Although reasonable minds continue to differ as to the necessity for—and desirability of—specific reforms, one of the more common themes of these discussions was the possibility of creating some kind of "special advocate," a security-cleared lawyer or group of lawyers to argue against the government in adversarial proceedings before the Foreign Intelligence Surveillance Court ("FISC"), the court charged with overseeing government surveillance undertaken pursuant to FISA.

- **Ars Technica: *"America's Most Secretive Court Invites its First Outsider"* https://arstechnica.com/tech-policy/2015/09/americas-most-secretive-court-invites-its-first-outsider**
  In September 2015, the FISC appointed Preston Burton, a well-known Washington, DC lawyer, to be the first of a total of five amici curiae—friends of the court—who will act as a sort of ombudsman or public advocate at the =FISC.

- **Office of the Director of National Intelligence: *"Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2016"* https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf**
  In June 2013, President Obama directed the IC to declassify and make public as much information as possible about certain sensitive U.S. government surveillance programs while protecting sensitive classified intelligence and national security information. Since then, the Director of National Intelligence ("DNI") has declassified and authorized the public release of thousands of pages of documents relating to the use of critical national security authorities. In addition to declassifying and publicly releasing these documents, the DNI and the IC have published four reports regarding these authorities. The most current report was issued in April 2017, and it provides the statistics relating to the use of critical national security authorities for the calendar year 2016.

- **Brennan Center for Justice at New York University School of Law: "*NO to DHS Social Media Password Requirement*" https://www.brennancenter.org/analysis/brennan-center-condemns-dhs-proposal-collect-social-media-passwords**
  The Brennan Center joined a coalition of civil liberties organizations, trade associations, and experts in condemning a Department of Homeland Security proposal to collect social media passwords from non-citizens as a condition for entrance to the United States.

- **Elizabeth Goitein: Brennan Center for Justice at New York University School of Law*: "The New Era of Secret Law"* https://www.brennancenter.org/sites/default/files/publications/The_New_Era_of_Secret_Law.pdf**

This document provides information about a growing body of "secret law" enacted without public scrutiny or Congressional input. It provides information about what constitutes secret law, its history, its legal and practical implications, and the differences between secret law and secret implementation, and the implication of the use of "secret laws" on the United States democracy.

- **National Security Agency, Civil Liberties and Privacy Office*: "NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 (April 16, 2017)"***
  https://fas.org/irp/nsa/clpo-702.pdf- This report was prepared by the National Security Agency ("NSA") Civil Liberties and Privacy Office as part of its responsibilities to enhance communications and transparency with the public and stakeholders. The intent of this paper is to help build a common understanding that can serve as a foundation for future discussions about the existing civil liberties and privacy protections while protecting the nation from terrorism.

- **Jack Goldsmith: Hoover Institute: "*A Partial Defense of the Front-Page Rule"***
  http://www.hoover.org/research/partial-defense-front-page-rule
  The essay analyzes the rule that states that the U.S. government should not engage in any secret, covert, or clandestine activity if it could not persuade the American people of the necessity and wisdom of such activities, were they to learn of them as the result of a leak or other disclosure. The corollary of that rule is that if a foreign government's likely negative reaction to a revealed collection effort would outweigh the value of the information likely to be obtained, then the collection should not be done either. This analysis is limited to "communications intelligence that takes place in the homeland or that affects US persons abroad."

- **EUROPEAN COMMISSION: *"European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows"***
  http://europa.eu/rapid/press-release_IP-16-2461_en.htm
  The EU-U.S. Privacy Shield is a robust new system to protect the personal data of Europeans and ensure legal certainty for businesses. It brings stronger data protection standards that are better enforced, safeguards on government access, and easier redress for individuals in case of complaints. The goal of the new framework is to restore the trust of consumers when their data is transferred across the Atlantic.

- **EUROPEAN COMMISSION: *"EU-U.S. Privacy Shield Fact Sheet"***
  http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf
  This document provides a short summary of the EU and U.S. Privacy Shield agreement.

- **EUROPEAN COMMISSION: *"ANNEXES to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield"***
  http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
  This document provides includes Seven Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. The annexes include: ANNEX I Letter from U.S. Secretary of Commerce Penny Pritzker; ANNEX II EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce; ANNEX III Letter

from U.S. Secretary of State John Kerry; ANNEX IV Letter from Federal Trade Commission Chairwoman Edith Ramirez; ANNEX V: Letter from U.S. Secretary of Transportation Anthony Foxx; ANNEX VI Letter from General Counsel Robert Litt, Office of the Director of National Intelligence; ANNEX VII Letter from Deputy Assistant Attorney General and Counselor for International Affairs Bruce Swartz, U.S. Department of Justice

- **Information Sharing Enterprise:** ***"Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment"***
  https://www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf
  This document provides guidelines that apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and federal laws of the United States.

- **Information Sharing Enterprise:** ***"Annual Report to the Congress" August 2016***
  https://www.ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf
  The 2016 Information Sharing Environment ("ISE") Annual Report to Congress provides information about three major lines of effort for improved implementation of the ISE: The three major lines of effort are Effort 1: Advance the terrorism-related ISE at the domestic nexus of public safety and national security; Effort 2: Develop and integrate Project Interoperability ("PI") and the Information Sharing and Safeguarding Core Interoperability Framework to improve information sharing and safeguarding by ISE partners across their enterprise architectures; and Effort 3: Support federal departments and agencies with their efforts to implement national information sharing objectives via the Strategic Implementation Plan ("SIP") published in 2013.