(U) Additional Unclassified Statement by Board Member Travis LeBlanc, March 12, 2021

(U) Introduction

(U) The Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board") was created to serve as an independent oversight Board to enhance the United States government's "system of checks and balances to protect the precious liberties that are vital to our way of life and to ensure that the Government uses its powers for the purposes for which the powers were given."[1] We are directed to ensure that privacy and civil "libert[ies] concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism."[2] We do this best when we conduct a thorough investigation, review records that corroborate or contradict an agency's oral representations, probe compliance infractions, rely upon evidence-based analysis to reach independent conclusions, identify technological and legal evolutions that are material to the program's lawfulness, and produce a report that is as transparent to the public as possible. Today's report, titled *Report on Certain NSA Uses of XKEYSCORE for Counterterrorism Purposes*, unfortunately fails these metrics.[3]

(U) It is with deep regret that I must write in opposition to the release of a report that the former majority of the Board in 2020 ("former Board" or "former Board majority") rushed last year to approve without adequate investigation, analysis, review, or process. While I remain grateful to our Board staff for the many years of effort they have devoted to XKEYSCORE's oversight, I had hoped that the former majority of the Board would have conducted a more thorough investigation of this highly-classified surveillance program that is unlikely to be scrutinized by another independent oversight authority in the near future.

(U) *First*, I voted against the XKEYSCORE report because the former Board majority failed to use its investigation into Executive Order ("EO") 12333 activities[4] to delve into important technological and modern electronic surveillance issues dominating the public discourse, like the use of algorithmic decision-making.

(U) *Second*, the former Board majority failed to adequately investigate or evaluate the National Security Agency's ("NSA") EO 12333 collection activities. Obviously, NSA can process and query communications through XKEYSCORE only once it has access to those communications. While collection and querying are separate activities, they are intertwined and both are worthy of review for separate legal analysis, training, compliance, and audit processes. This is true whether the collection and querying activities are performed by humans or machines. What may be a reasonable amount of "incidental" collection in one program or activity may well be

---

[1] (U) 42 U.S.C. § 2000ee(b)(2).
[2] (U) 42 U.S.C. § 2000ee(c)(2).
[3] (U) PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON CERTAIN NSA USES OF XKEYSCORE FOR COUNTERTERRORISM PURPOSES (2020) ("NSA Deep Dive").
[4] (U) Executive Order 12333 ("EO 12333"), 46 Fed. Reg. 235 (Dec. 8, 1981). EO 12333 establishes a framework that applies broadly to the government's collection, analysis, and use of foreign intelligence and counterintelligence—from human sources, by interception of communications, by cameras and other sensors on satellite and aerial systems, and through relationships with intelligence services of other governments. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, EXECUTIVE ORDER 12333 3 (2020).

(b) (1)
(b) (3)-P.L. 86-36

unreasonable in other contexts.[5] Similarly, protections that are designed to mitigate incidental collection may be reasonable in one program or activity and unreasonable in other contexts. On these points and others, the former Board's report unfortunately reads more like a book report summary of the XKEYSCORE program than an independent oversight analysis grappling with key concerns in this evolving technological and legal landscape.

(U) *Third*, the former Board majority had the opportunity to engage in evidence-based policy making; however, it concluded a report lacking analysis of the efficacy, costs, and benefits of XKEYSCORE.

~~(TS//SI//NF)~~ *Fourth*, the former Board majority failed to adequately investigate the compliance program in place for XKEYSCORE. Unfortunately, when the former Board requested any legal analysis by the NSA or the Department of Justice ("DOJ") regarding the use of XKEYSCORE's functions in 2015, the NSA provided a 13-page memo prepared by the NSA Office of General Counsel ("OGC") in 2016.[6] The response made it appear as if NSA had not prepared a written analysis of the legality of XKEYSCORE until prompted by PCLOB.[7] The memo touches on the Fourth Amendment and a number of statutory regimes; however, it fundamentally rests on dated case law.[8] In addition, there was no mandatory XKEYSCORE-specific training for NSA analysts, nor did the former Board agree to follow up on any of the [redacted] of compliance incidents that were reported to us.[9] NSA reported, for example, that in 2019, there were [redacted] compliance reports and that [redacted] these were deemed to constitute "Questionable Intelligence Activities"—a term used by the Department of Defense ("DOD") to signify that an action may have resulted in illegal surveillance or improper review of U.S. person communications.[10] But the former Board refused to inquire into any of these compliance incidents or [redacted] U.S. person XKEYSCORE queries before issuing this report.[11]

---

[5] (U) *See e.g.*, the surveillance conducted under a traditional wiretap as opposed to "upstream surveillance." DAVID KRIS AND J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 3:2 (3rd. ed. 2019); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 7-8 (2014).

[6] (U) Nat'l Sec. Agency, *Legal Analysis of XKEYSCORE*, Jan. 20, 2016 at 1 ("NSA Legal Analysis").

[7] (U) The former Board asked NSA to provide any "[l]egal analysis by the NSA and Department of Justice regarding the use of XKEYSCORE's analytic functions and its consistency with statute, executive order, and the Constitution." PCLOB Document Request to NSA, Dec. 15, 2015. The NSA responded with a 13-page document drafted in 2016 and noted that it was "based on [Office of the General Counsel's (OGC's)] previous internal legal analyses." *See* NSA Legal Analysis at 1. Upon reviewing my separate statement in March 2021, the NSA shared with me for the first time that they purport to have prior legal analyses of XKEYSCORE other than legal analyses by OGC to NSA personnel regarding discrete legal issues. The full Board and I have requested these purported legal analyses. We have not been provided them as of the publishing of this statement. *See* Member Travis LeBlanc's Counsel Mark M. Jaycox in discussion with NSA's Director of Civil Liberties and Privacy Rebecca J. Richards, Mar. 17, 23, and 30, 2021; Member Travis LeBlanc's Counsel Mark M. Jaycox, email messages to NSA's Director of Civil Liberties and Privacy Rebecca J. Richards, Mar. 15, 19, 24, 30, Apr. 5, and May 7, 2021; Privacy and Civil Liberties Board, email message to NSA's Director of Civil Liberties and Privacy Rebecca J. Richards, Jun. 22, 2021.

[8] (U) *See generally* NSA Legal Analysis.

[9] (U) NSA Deep Dive at 35 n.72 and 73.

[10] (U) Questionable Intelligence Activities (QIA) defined as "any intelligence or intelligence-related activity when there is reason to believe such activity is unlawful or contrary to an EO, Presidential Directive, [Intelligence Community] Directive, or applicable DOD policy governing the activity." Dep't of Defense, *DOD Directive 5148.13: Intelligence Oversight* 16 ("DOD Directive 5148.13").

[11] (U) In the interest of transparency, I note that the NSA requested these redactions. While I do not

(U) *Fifth*, I have joined fellow Board Member Ed Felten in offering three additional recommendations that the former Board majority voted to exclude from the report.[12] These are important recommendations that should have been included in the report.

(U) *Sixth*, the former Board majority has also failed in its mission to inform the public about our work. Our authorization statute directs us to make our reports, including our reports to Congress, "available to the public to the greatest extent that is consistent with the protection of classified information and applicable law."[13] Here, the former Board majority has made no effort to seek declassification of the report, any portions thereof, or any materials that the Board reviewed. This is inexcusable.

(U) *Lastly*, I have serious concerns about the unconventional process that the former Board majority followed to approve and release this report. To be clear, despite my repeated requests, the current 2021 Privacy and Civil Liberties Oversight Board has not voted to release this report nor to include the statement of a former member.[14] The result is that today the former Board majority releases an inadequate report that reflects its failure to engage in effective oversight.

(U) I have provided a more fulsome explanation of my concerns with the XKEYSCORE report in my classified statement, but I believe that it is equally important to share some of these concerns in this unclassified statement. Unfortunately, I will not be able to detail many of my concerns in this unclassified statement. I have, however, worked with the appropriate authorities to make this statement as transparent and public as possible.

(U) Despite my concerns with the former Board majority's report, the professional staff at PCLOB must be commended for their diligent, hard-working, and proficient work. They were critical to moving this report forward (particularly during those years in which we were inquorate), and I join my fellow Board Members in thanking them for their professionalism and their dedication to the Board's mission.[15]

(U) 21st Century Issues Demand 21st Century Investigations

(U) *First*, the former Board's review of EO 12333 activities presented an opportunity to address modern surveillance capabilities and privacy and civil liberties harms dominating the public discourse. For instance, modern electronic surveillance touches on pioneering uses of artificial intelligence/machine learning (AI/ML) systems, including autonomous collection of massive datasets, analysis of those massive datasets through algorithmic decision-making, and many other AI/ML issues.[16] Whether the public wants it or not, these systems are almost certainly here

---

believe this information should remain classified, I will continue to work with the agency to seek public interest declassification.

[12] (U) NSA Deep Dive at 50-51.

[13] (U) 42 U.S.C. § 2000ee(f)(1).

[14] (U) *See* Member Travis LeBlanc, email messages to members of the Privacy and Civil Liberties Oversight Board, Feb. 11, 18, 19, 20, and 24, 2021; *See also* Board Meeting of the Privacy and Civil Liberties Oversight Board, Mar. 5, 2021.

[15] (U) I also want to express my profound gratitude to my Counselor, Mark M. Jaycox. Since arriving at PCLOB, Mark has worked tirelessly with me on my classified and unclassified statements. I commend him for his steadfast counsel and commitment to the Board's mission.

[16] (U) John Nay & Katherine J. Strandburg, GENERALIZABILITY: MACHINE LEARNING AND HUMANS-IN-THE-LOOP, RESEARCH HANDBOOK ON BIG DATA LAW, (Roland Vogl. ed., Elgar Publishing 2021); Solon Barocos, dana boyd, Sorelle Friedler, and Hannah Wallach, *Social and Technical Trade-Offs in Data Science*, 5 BIG DATA 2 71-72 (2017); Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the*

to stay. Although the lion's share of modern surveillance is done by machines, these surveillance tools are created by humans, implemented by humans, and directed by humans. Competent overseers must begin to grapple with critical questions about modern electronic surveillance like the appropriate role of algorithmic decision making, how data is categorized or tagged, the weight ascribed to certain data, how classes of communications are prioritized, and the all too familiar concept of AI/ML "black boxes."[17] Other issues to grapple with include: the extent to which a machine analysis of U.S. person information triggers Fourth Amendment scrutiny (as opposed to a "human-eyes" review); how modern surveillance technology implicates the Fourth Amendment; the Mosaic Theory of the Fourth Amendment; the challenges to the "incidental overhear" doctrine when evaluating the reasonableness of Big Data surveillance; the lack of a Supreme Court-recognized foreign intelligence exception to the Fourth Amendment's warrant requirement; and, many more.[18]

(U) Every project we conduct should be an opportunity to explore these issues and determine whether they are applicable and need further analysis. It is disappointing that the report failed to address these topics—especially when so many external stakeholders have sought the Board's considered insight on these issues.[19]

(U) A Failure to Investigate: The Full Scope of Signals Intelligence

(U) *Second*, I voted against the XKEYSCORE report because the former Board majority failed to adequately investigate or evaluate NSA's collection activities. XKEYSCORE is used by NSA personnel "to execute signals intelligence responsibilities assigned to the Agency by EO 12333. .

Fourth Amendment, 164 U. PENN. L. REV. 871 (2016); Tal Z. Sarsky, *Transparent Predictions*, 4 U. ILL. L. REV. 1519-20 (2013). These causes for concern are exacerbated by the fact that AI/ML is capable of improving itself, resulting in a feedback loop that may potentially advance its own intelligence beyond its human developers. *See e.g.*, NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 124-5 (2014).

[17] (U) For an introduction to the Black Box problem and other aspects *see generally* FRANK PASQUELE, BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015). *See also* Danielle Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

[18] (U) *See generally* Steven Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for Int'l Peace, Sept. 17, 2019; Tal Z. Sarsky, *Transparent Predictions*, 4 U. ILL. L. REV. 1519-20 (2013); Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PENN. L. REV. 871 (2016); Orin S. Kerr, *The Mosaic Theory and the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); Orin S. Kerr, *Implementing Carpenter*, USC Law Legal Studies Paper 18-29, Dec. 14, 2018; Paul S. Ohm, *The Many Revolutions of* Carpenter, 32 HARVARD J. OF L. AND TECH. 373 (2019); Danielle Citron and David Gray, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Elizabeth Goitein, *Another Bite out of* Katz: *Foreign Intelligence Surveillance and the "Incidental Overhear" Doctrine*, 55 AMERICAN CRIM. L. REV. 105 (2018). It is also worth noting that even if the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review have concluded there is a foreign intelligence exception to the Fourth Amendment's warrant requirement when electronic surveillance is undertaken for foreign intelligence purposes, those courts are not adversarial and any ruling must be placed in that context. Both courts did not hear from *amici* until 2015 with the passage of the USA Freedom Act. USA Freedom Act of 2015, PUB. L. NO. 114-23, tit. IV, § 401 (2015). *See also Statement of Former Board Member Aditya Bamzai* at 16 n.88; *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1010 (F.I.S.C.R. 2008).

[19] (U) *See e.g.*, ACLU, *Letter dated Jan. 13, 2016 to Privacy and Civil Liberties Oversight Board*, Jan. 13, 2016; Brennan Center for Justice at NYU Law, *Letter dated Jun. 16, 2015*, Jun. 16, 2015; Center for Democracy and Technology, *Comment to the Privacy and Civil Liberties Oversight Board Regarding Reforms to Surveillance Conducted Pursuant to Executive Order 12333*, Jun. 16, 2015; Electronic Privacy Information Center, *Letter dated Jun. 16, 2015*, Jun. 16, 2015; Reporters Committee for Freedom of the Press, *Letter dated Jun. 16, 2015*, Jun. 16, 2015; Open Technology Institute, *Letter dated Jun. 15, 2015*, Jun. 15, 2015.

.and other applicable law and policy direction."[20] XKEYSCORE is also described as a "processing and discovery system"[21] and "analytic" tool.[22] It is beyond obvious that NSA must gather or collect that signals intelligence from somewhere—in the United States or abroad.[23] The former Board majority declined to review the agency's collection activities. I disagree with that decision to focus the report only on the analytical capabilities of XKEYSCORE. As a result, the former Board failed to properly scope its investigation and left critical facts unexplored.

(U) The distinctions between discovery, targeting, and acquisition are well-known concepts in electronic surveillance.[24] These concepts are complex and our electronic surveillance law has not kept pace with the current surveillance capabilities of the government or with the new privacy and civil liberties harms that may result from use of modern surveillance tools. The former Board approached this report by collapsing distinct concepts like discovery, targeting, and acquisition as well as failing to probe critical technical, legal, and constitutional issues. In many instances, the former majority simply regurgitates NSA's own analysis or talking points on legal and constitutional issues, or disregards modern judicial precedent.[25]

(U) A Failure to Investigate: Cost-Benefit Analysis and Efficacy of the Program

(U) *Third*, it is basic that oversight of a government program should include an evaluation of the efficacy of the program, including at least an analysis of its costs and benefits.[26] I voted against the report because the former Board majority failed to evaluate the efficacy of XKEYSCORE through a cost-benefit analysis or otherwise. In the past, the Board has included an efficacy analysis in all three of the major oversight reports that we have released.[27] The former Board

---

[20] (U) NSA Legal Analysis.
[21] (U) NSA Deep Dive at 3.
[22] (U) PCLOB Examination of EO 12333 Activities in 2015, available at https://documents.pclob.fov/prod/Documents/EventsAndPress/b7b559bb-6687-4638-a7af-f40f2f9ae09a/20150408-EO12333_Project_Description.pdf.
[23] (U) For the history on where the U.S. government located fixed intercept stations and communications intelligence sites in U.S. territories *see* Nat'l Sec. Agency, *COMINT Stations Overseas*, https://www.nsa.gov/about/cryptologic-heritage/center-cryptoloic-history/pearl-harbor-review/comint/.
[24] (U) Nat'l Sec. Agency, *Signals Intelligence,* May 3, 2016, https://www.nsa.gov/what-we-do/signals-intelligence. *See* Nat'l Sec. Agency, *United States Signals Intelligence Directive SP0018: Legal Compliance and U.S. Persons Minimization Procedures*, Jan. 25, 2011 ("USSID 18"); EO 12333 at § 2.3; DAVID KRIS AND J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS (3rd. ed. 2019); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT (2020); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014).
[25] (U) *See e.g.*, NSA Deep Dive Report Part IV titled "NSA's Analysis of XKEYSCORE." NSA Deep Dive at 42.
[26] (U) Council of the Inspectors General on Integrity and Efficiency, *Quality Standards*, https://www.ignet.gov/content/quality-standards.
[27] (U) PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 127, 146-155 (2014); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 158 (2014); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 63 (2020).

majority failed to ask critical questions like how much the program costs financially to operate, how many U.S. persons have been impacted by XKEYSCORE, how much data the program collects and analyzes, how widely information analyzed through XKEYSCORE is shared, the number of lives saved, or the number of terrorist events averted as a result of XKEYSCORE. Instead, the former Board majority included only anecdotal evidence in the report drawn from briefings by NSA. The former Board majority should have investigated any potential metrics, variables, or key computational questions concerning the efficacy and effectiveness of XKEYSCORE. Unfortunately, the former Board majority did not. The former Board majority included just two counterterrorism examples of the "Operational Value" of the program, despite one former Member's conclusion that the tool was "powerful, ingenious, adaptable, and customizable."[28]

(U) Effective oversight necessitates a robust investigation into the efficacy of the programs we oversee. The Board's former majority has failed to do that. We should not have prematurely terminated our investigation of efficacy to rush to a vote on this report before the end of 2020.[29] The former Board, should have engaged with the metrics, variables, and key computational questions concerning the efficacy and effectiveness of this powerful surveillance tool.[30] Unfortunately, that evidence-based policy analysis did not occur.

(U) XKEYSCORE Compliance Deficiencies

(U) *Fourth*, I voted against the report because the former Board majority sought to issue it without completing diligence on NSA's compliance efforts, including its legal analysis, policies, training, compliance, and auditing.

(U) A primary step in developing any compliance program is a legal analysis of the program.[31] The legal analysis that sets forth the authorities and limitations of a program typically forms the foundational basis necessary for the development of compliance policies and procedures. Surprisingly, when the Board requested any legal analysis by the NSA or the Department of Justice regarding the use of XKEYSCORE's functions in 2015, the NSA responded with a 13-page memo prepared by the NSA Office of General Counsel in 2016.[32] Setting aside such a legal analysis was first written in January 2016, it is equally concerning that the agency apparently has not updated that written legal analysis since then.[33] At a general level and on the basis of the documents that have been provided to the Board, it is concerning that any surveillance tool would have been conceptualized, coded, implemented, and then executed and routinely used without such a prior written legal analysis.[34] Further, the analysis that NSA provided in 2016 fundamentally rests on decades-old Supreme Court precedent from *United States v. Verdugo-Urquidez*, *Smith v. Maryland*, *Katz v. United States*, and two DOJ legal memoranda from the 1980s to assert that collection and use of XKEYSCORE is consistent with the Fourth Amendment.[35] The NSA's legal analysis lacks any consideration of recent relevant Fourth

---

[28] (U) *Additional Views by Chairman Adam Klein* at 1.
[29] (U) Privacy and Civil Liberties Oversight Board Meeting, Dec. 16, 2021.
[30] (U) *Additional Views by Chairman Adam Klein* at 1.
[31] (U) *See generally* INT'L ASSN. OF PRIVACY PROFESSIONALS, PRIVACY PROGRAM MANAGEMENT (2nd. ed. 2019); Nat'l Institute of Standards and Tech., *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, 11 (Jan. 16, 2020).
[32] (U) *See supra* n.7.
[33] (U) NSA Legal Analysis.
[34] (U) *Id.*
[35] (U) *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990); *Smith v. Maryland*, 442 U.S. 735 (1979);

(b) (1)
(b) (3)-P.L. 86-36

Amendment case law on electronic surveillance that one would expect to be considered—for example *Carpenter v. United States, Riley v. California, United States v. Jones, and United States v. Maynard.*[36]

(U) Given the apparent lack of such a written legal analysis prior to our investigation, it should come as no surprise that NSA does not currently require analysts to receive privacy and civil liberties compliance training tailored specifically to XKEYSCORE.[37] One would have expected that there would be mandatory, robust compliance training specific to XKEYSCORE given how powerful of a tool it is and according to NSA's own publicly-accessible framework for compliance.[38]

~~(TS//SI//NF)~~ I am equally concerned that the Board's former majority failed to investigate [redacted] of serious compliance reports involving XKEYSCORE prior to approving this report.[39] During the former Board's investigation, it was uncovered in November 2020 that some [redacted] compliance reports involving XKEYSCORE occurred in 2019.[40] Of those [redacted] XKEYSCORE reports, [redacted] were deemed upon agency review to involve Questionable Intelligence Activities ("QIAs").[41] QIAs are defined as "any intelligence or intelligence-related activity when there is reason to believe such activity is unlawful or contrary to an EO, Presidential Directive, [Intelligence Community] Directive, or applicable DOD policy governing the activity."[42] To be clear, ove [redacted] of reports in a one-year period involved QIAs.[43] Obviously, violations of U.S. law and the known collection or processing of U.S. person information are serious compliance issues. Yet, the former Board did not request specific information on any of these QIAs, nor did the former Board request equivalent data about compliance incidents in any other years.

Katz v. United States, 389 U.S. 347 (1967).

~~(TS//SI//NF)~~ [redacted]

[36] (U) *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).
[37] (U) NSA Deep Dive at 35.
[38] (U) Nat'l Sec. Agency, *Essential Elements of a Compliance Program*, Jun. 24, 2016, https://nsa.gov/Portals/70/documents/about/civil-liberties/resources/essential-elements-of-a-compliance-program.pdf.
[39] (U) The behavior is in stark contrast to the former Board's approach in its 2020 *Report on the Government's Use of the Call Detail Records Program Under the USA Freedom Act* where it engaged in rigorous analysis into the efficacy of the program. There, the Board dedicated an entire section of the report to discuss compliance incidents: "Root Causes of the Compliance Incidents and Date Integrity Challenges." PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 63 (2020). *See also* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 127, 146-155 (2014); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 158 (2014).
[40] (U) PCLOB Questions received on September 14, 2020 regarding XKEYSCORE Deep Dive, Answer 2(b)(i), Sept. 14, 2020; See also NSA Briefing on XKEYSCORE (Feb. 7, 2019).
[41] (U) PCLOB Questions received on September 14, 2020 regarding XKEYSCORE Deep Dive, Sept. 14, 2020.
[42] (U) DOD Manual 5148.13 at 16.
[43] (U) *See supra* n.38.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36
(b) (5)

(b) (1)
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ The lack of satisfactory legal analysis, insufficient training, [redacted] of uninvestigated compliance reports, and the former Board's inability to otherwise investigate critical privacy and civil liberties issues all shine poorly on the former Board's credibility and ability to conduct itself as an oversight body.

(U) The Board Failed to Adopt the Former Minority Recommendations

(U) *Fifth*, I have joined fellow Board Member Ed Felten in offering three additional recommendations for inclusion in the report.[44] These recommendations address the treatment of U.S. person information and 21st century challenges around encrypted communications. These three important recommendations should have been adopted by the full Board.

(U//~~FOUO~~) Specifically on one recommendation, I join Member Felten's discussion of our additional recommendations in his classified separate statement and also note that while inadvertently or incidentally intercepted communications of U.S. persons is a casualty of modern signals intelligence, the mere inadvertent or incidental collection of those communications does not strip affected U.S. persons of their constitutional or other legal rights.[45] Even NSA's Legal Compliance and Minimization Procedures (United States Signals Intelligence Directive SP0018) recognize that inadvertently collected U.S. person communications "will be promptly destroyed upon recognition, if technically possible" (except in a few enumerated circumstances such as a threat of death or serious bodily harm).[46] Setting aside whether known U.S. person communications should be retained at all, Member Janie Nitze apparently takes issue with the minor effort that it would take for an analyst to tag data known or believed to constitute U.S. person information [redacted] that may be retained and queried for five years (as of now).[47] Member Nitze does not argue that the tagging requirement she opposes would be unreasonable or unduly burdensome on analysts.[48] Nor could she. The recommendation does not require NSA analysts to take any actions in seeking to identify U.S. person information, nor does it require NSA to substantively amend its minimization procedures.[49] But as the NSA has itself explained, "NSA is required by its Attorney General approved minimization procedures to make reasonable efforts to reduce to the maximum extent practicable the number of non-foreign communications acquired during SIGINT operations."[50] The creation and use of a U.S. person information tag is clearly reasonable and this is particularly so when the objective is to reduce the collection and retention of U.S. person communications to the *maximum extent possible*.

(b) (3)-P.L. 86-36

[44] (U) NSA Deep Dive at 50-51.
[45] (U) U.S. v. *Warshak*, 631 F.3d 266 (2010); *Berger v. New York*, 388 U.S. 41, 59 (1967); *Katz v. United States*, 389 U.S. 347 (1967); 18 U.S.C. § 2518; 50 U.S.C. § 1805, § 1824. It's important to note that these cases and more modern cases are in the context of two-party communications and the Supreme Court has yet to grapple with the relevant Constitutional merits. *See United States v. Kahn*, 415 U.S. 143 (1974); United *States v. Donovan*, 429 U.S. 413 (1977); *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019); *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016).
[46] (U) Nat'l Sec. Agency, *United States Signals Intelligence Directive SP0018: Legal Compliance and U.S. Persons Minimization Procedures* § 5.4(b)(1), Jan. 25, 2011 ("USSID 18").
[47] (U) *Statement of Board Member Janie Nitze* at 1.
[48] (U) *Statement of Board Member Janie Nitze* at 1.
[49] (U) NSA Deep Dive at 50-51.
[50] (U) NSA Legal Analysis at 7.

(U) The Board Failed the Public

(U) *Sixth*, the former majority of the Board has also failed in its mission to inform the public about our work. Our authorization statute directs us to make our reports, including our reports to Congress, "available to the public to the greatest extent that is consistent with the protection of classified information and applicable law."[51] Here, the Board has made no effort to seek declassification of this report, any portions thereof, or any materials that the Board reviewed. This is inexcusable.

(U) In addition to our statutory mandate, there are very good policy reasons for why our Board's activities should be as transparent as possible. Transparency encourages accountability. When PCLOB publicly releases its reports, it allows the public and other external stakeholders to engage with material that is often kept under classification and out of the public eye. It allows academics and journalists to further investigate potentially wasteful or unlawful government surveillance. It allows civil society to advocate for new policy positions. And it allows Congress to further oversee and legislate changes to the law. All of these actions engender public trust that there is sufficient and adequate oversight of national security programs and activities.

(U) Transparency also encourages credibility. A thorough report increases PCLOB's credibility to provide constructive criticism to agencies engaged in practices with a potential for significant privacy and civil liberties harms. It also encourages credibility in NSA itself as the agency listens, responds, and incorporates feedback—not just from the Board, but from an informed democracy.

(U) The public is rightfully worried about secret surveillance programs. By being transparent with our reports and activities, PCLOB ensures the public understands oversight is occurring and that privacy and civil liberties harms are being addressed. It is unfortunate the Board has failed to seek declassification of even discrete sections of the NSA report. As we have been directed by Congress, I urge the Board to request declassification of its report and release as much information to the public "to the greatest extent that is consistent with the protection of classified information and applicable law."[52]

(U) Procedural Issues Plague the Report's Release

(U) Finally, I have several concerns about the Board process that was followed to apparently approve the unfinished report. In a December 2020 Board meeting, the former majority sought to vote on the then-unfinished XKEYSCORE report.[53] During the Board meeting at which the vote was taken, we spent several hours discussing the revisions to the body and recommendations that would need to be made to the report. Instead of completing those revisions and then providing sufficient time for Members to review the report and prepare their statements before voting, the former Board majority sought in that meeting to approve the report for this project, ostensibly foreseeing the expiration of former Member Aditya Bamzai's term at the end of December. Literally on the evening of December 31, former Member Bamzai circulated his statement. Subsequently, the new Board convened in January 2021 and the then-Chairman submitted his own intention to resign the same month.[54] Recognizing that the current

[51] (U) 42 U.S.C. § 2000ee(f)(1).
[52] (U) *Id.*
[53] (U) Board Meeting of the Privacy and Civil Liberties Oversight Board, Dec. 16, 2020.
[54] (U) Privacy and Civil Liberties Oversight Board, *Statement by Chairman Adam I. Klein on Intent to Resign as Chairman of the Privacy and Civil Liberties Oversight Board*, Jan. 25, 2021.

2021 Board has not voted on a report that we were still considering for revision as I drafted this statement, I have repeatedly requested a vote by the current Board on the final version of this report, including all final statements of current Members as well as a vote on whether to include the statement of a former Member.[55] The then-current Chairman created a legal fiction to compel the issuing of a former Member's statement without so much as a vote of the current Board to release this report.[56] I simply cannot support a report that has not been voted on by the current Board that will issue it.

(U) Conclusion

(U) For these reasons and others included in my classified statement, I am unable to support the former Board's report on the XKEYSCORE program. I harbor serious reservations about the deficiencies in our oversight of the XKEYSCORE program as well as significant concerns about the program's operations. I hope the deficiencies and gaps identified in my statements will help provide guidance to NSA on additional issues that it needs to address with respect to the operations of XKEYSCORE. I also hope that the issues raised in these statements inspire a future PCLOB to more effectively perform its oversight and advising functions when assessing other surveillance programs.

[55] (U) Board Member Travis LeBlanc, email messages to members of the Privacy and Civil Liberties Oversight Board, Feb. 11, 18, 19, 20, and 24, 2021; *See also* Board Meeting of the Privacy and Civil Liberties Oversight Board, Mar. 5, 2021.

[56] (U) Board Meeting of the Privacy and Civil Liberties Oversight Board, Mar. 5, 2021.