

[ORAL ARGUMENT NOT YET SCHEDULED]

No. 25-5197

**IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

TRAVIS LEBLANC; EDWARD FELTEN

Plaintiffs-Appellees

v.

U.S. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, et al.

Defendants-Appellants

On Appeal from the U.S. District Court
for the District of Columbia, No. 1:25-cv-00542-RBW
(Hon. Reggie B. Walton)

**BRIEF OF PETER SWIRE AS AMICUS CURIAE SUPPORTING
PLAINTIFFS-APPELLEES**

Professor Peter Swire
Counsel of Record
2026 Castleway Lane NE
Atlanta, GA 30345
(240) 994-4142
peter@peterswire.net

September 12, 2025

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), amicus curiae Peter Swire hereby certifies as follows:

(A) Parties and amici.

Except for the *amicus* submitting this brief and *amici* who submitted briefs in the days since the parties' briefs, all parties, intervenors, and *amici* appearing before the district court and this Court are listed in the Brief for Plaintiffs-Appellees and Briefs for Defendants-Appellants. The additional *amici* are listed on this Court's docket.

(B) Ruling under review.

The rulings at issue before this Court appear in the Brief for Plaintiffs-Appellees and Briefs for Defendants-Appellants.

(C) Related cases.

This case has not previously been before this Court. Except for the cases identified in the Brief for Plaintiffs-Appellees and Briefs for Defendants-Appellants, counsel are unaware of any related cases within the meaning of Circuit Rule 28(a)(1)(C).

Dated: September 12, 2025

/s/ Peter Swire
Peter Swire

Counsel of Record

TABLE OF CONTENTS

INTEREST OF THE AMICUS CURAE.....	1
INTRODUCTION AND SUMMARY OF ARGUMENT	1
ARGUMENT	3
I. The PCLOB is a Unique Agency to Address the Fundamental Constitutional Tension Between Liberty and Security.....	3
A. The PCLOB Plays a Unique Role in Responding to the History of Constitutional Violations Under Secret U.S. Government Surveillance Programs	3
B. The Independence of the PCLOB is Clearly Established by the History of its Founding Statute	7
II. The History of PCLOB’s Statute is Legally Relevant in Determining its Independence.....	9
III. There is a Distinct Fourth Amendment Analysis for Secret Foreign Intelligence Surveillance, Supporting the Independence of the PCLOB	11
A. The PCLOB Oversees Reasonableness of the Fourth Amendment, But Not the Warrant Requirement.....	11
B. Changes in Technology and Surveillance Targets are an Important Feature of Secret Government Surveillance.....	14
C. Independence of the PCLOB Protects Fourth Amendment Reasonableness and is Constitutionally Relevant to this Case	17
IV. The Independence of the PCLOB is a Vital Aspect of the Statutory Structure and Function of the PCLOB.....	19
A. Additional Points Supporting the View that Congress and the Courts Rely on PCLOB’s Independence as Essential to its Structure and Function.....	20
B. The Longstanding and Previously-Unbroken U.S. Government Position is	

that the PCLOB is Independent	21
i. The U.S Government and European Legal Authorities Have Emphasized the Independence of the PCLOB	23
CONCLUSION	27

TABLE OF AUTHORITIES

Cases

<i>Brigham City v. Stuart</i> , 547 U.S. 398 (2006).....	13
Case C-288/12, <i>Eur. Comm'n v. Hungary</i> , ECLI:EU:C:2014:237 (Apr. 8, 2014)	24
Case C-311/18, <i>Data Prot. Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems</i> , ECLI:EU:C:2020:559 (Jul. 16, 2020).....	23
Case C-362/14, <i>Maximillian Schrems v. Data Prot. Comm'r</i> , ECLI:EU:C:2015:650 (Oct. 6, 2015).....	23
Case T-533/32, <i>Philippe Latombe v. European Comm'n</i> , ECLI:EU:T:2025:831 (Gen. Ct. Sept. 3, 2025).....	25
Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1	25, 26
Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection under the EU-US Data Privacy Framework, 2023 O.J (L 231) 118	24, 25
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983).....	18
<i>In re Certified Question of L.</i> , 858 F.3d 591 (Foreign Int. Surv. Ct. Rev. 2016).....	14
<i>Katz v. U.S.</i> , 389 U.S. 347 (1967).....	12
<i>LeBlanc v. U.S. Priv. & C.L. Oversight Bd.</i> , No. 25-cv-542, 2025 WL 1454010 (D.D.C. May 21, 2025)	20

<i>Maryland v. King</i> , 569 U.S. 435 (2013).....	14
<i>Redacted</i> , 402 F. Supp. 3d 45 (Foreign Intel. Surv. Ct. 2018).....	18
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	13
<i>United States v. Hasbajrami</i> , 945 F.3d 641 (2d Cir. 2019)	6
<i>United States v. Mohamud</i> , 843 F.3d 420 (9th Cir. 2016)	6
<i>United States v. Muhtorov</i> , 20 F.4th 558 (10th Cir. 2021)	6
<i>United States v. United States District Court</i> , 407 U.S. 297 (1972).....	12
<i>Vernonia Sch. Dist. 47J v. Acton</i> , 515 U.S. 646 (1995).....	14
<i>Weiner v. U.S.</i> , 357 U.S. 349 (1958).....	9
<i>Wyoming v. Houghton</i> , 526 U.S. 295 (1999).....	14
 <u>Statutes</u>	
42 U.S.C. § 2000ee	14, 18
50 U.S.C. § 1805.....	13
Pub. L. No. 110-261, 122 Stat. 2436, 118th Cong. (2008).....	16
Pub. L. No. 114-23, H.R. 2048, 114th Cong. (2015)	7

Pub. L. No. 115-118, 132 Stat. 3, 115th Cong. (2018).....	21
---	----

Other Authorities

Alison A. Bradley, <i>Extremism in the Defense of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT ACT</i> , 77 TUL. L. REV. 465 (2002).....	12
---	----

Article 29 Data Protection Working Party, <i>Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision</i> , WP 238 (Apr. 13, 2016)	25
---	----

Calvin Massey, <i>Two Zones of Prophylaxis: The Scope of the Fourteenth Amendment Enforcement Power</i> , 76 GEO. WASH. L. REV. 1 (2007).....	10
---	----

Charley Savage and Luke Broadwater, <i>House Passes Two-Year Surveillance Law Extension Without Warrant Requirement</i> , N.Y. TIMES, Apr. 12, 2024, https://www.nytimes.com/2024/04/12/us/politics/surveillance-bill-fisa.html	21
--	----

European Data Protection Board, <i>Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework</i> (Feb. 28, 2023)	25
---	----

Exec. Order No. 13636, 78 Fed. Reg. 11739	22
--	----

Exec. Order No. 14086, 87 Fed. Reg. 62283	22
--	----

Fabiola Carrion, <i>Cautious Optimism as US Privacy Oversight Board Finally Confirms Chair</i> , ACCESS NOW (Jan. 12, 2023), https://www.accessnow.org/cautious-optimism-as-us-privacy-oversight-board-finally-confirms-chair	6
--	---

<i>Final Report of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities</i> , S. Rep. No. 755, 94th Cong., 2d Sess. (April 29, 1976).....	3
--	---

Jack Beerman, <i>A Critical Approach to Section 1983, With Special Attention to Sources of Law</i> , 42 STANF. L. REV. 51 (1989).....	10
---	----

MORTON H. HALPERIN ET AL., <i>THE LAWLESS STATE: THE CRIMES OF THE U.S. INTELLIGENCE AGENCIES</i> (1976).....	3, 4
PCLOB, Press Release, Statement by Chairman Adam I. Klein on Intent to Resign as Chairman of the Privacy and Civil Liberties Oversight Board (Jan. 25, 2021), https://documents.pclob.gov/prod/Documents/EventsAndPress/27d46947-d630-4d9d-83df-109f567cc0b0/Chairman%20Intent%20to%20Resign%20Jan%2025_21.pdf ..	22, 23
PCLOB, <i>Recommendations Assessment Report</i> (Feb. 5, 2016), https://documents.pclob.gov/prod/Documents/OversightReport/8ab510df-738f-44b5-a73a-08d1336d544d/Recommendations_Assessment_Report_20160205%20-%20Completed%20508%20-%2010252022.pdf	7, 17
PCLOB, <i>Recommendations Assessment Report</i> (Jan. 29, 2015), https://documents.pclob.gov/prod/Documents/OversightReport/a97a9918-775d-42eb-b426-2ae01838c2a3/Recommendations_Assessment-Report_2015%20-%20Complete%20-%20Nov%202%202022%201544.pdf	5, 17
PCLOB, <i>Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act</i> (Jul. 2, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%2014%202022%201548.pdf	13, 17, 21
PCLOB, <i>Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act</i> (Sept. 28, 2023), https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20(002).pdf .	5, 13
PCLOB, <i>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</i> (Jan. 23, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf	5, 10

Peter Margulies, <i>Searching for Federal Judicial Power: Article III and the Foreign Intelligence Surveillance Court</i> , 85 GEO. WASH. L. REV. 800, 843 (2017), https://core.ac.uk/download/pdf/212910171.pdf	17
Peter Swire, <i>From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud</i> , 2 INT’L DATA PRIVACY L. 200 (2012)	17
Peter Swire, <i>The System of Foreign Intelligence Surveillance Law</i> , 72 GEO. WASH. L. REV. 1306 (2004)	3, 4, 12
Peter Swire, <i>The USA FREEDOM Act, the President’s Review Group and the Biggest Intelligence Reform in 40 Years</i> , IAPP, (Jun. 8, 2015), https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years/	7
Peter Swire, <i>U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013</i> , (Dec. 18, 2015), https://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf	15
Press Release, U.S. Dep’t of Just., Justice Department Statement on the European Union’s Adoption of Trans-Atlantic Data Privacy Framework to Restore Trust and Stability to Transatlantic Data Flows, Reflecting the Strength of EU-U.S. Relationship (Jul. 10, 2023).....	24
<i>Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies</i> , Liberty and Security in a Changing World (2013).....	4, 6, 15

INTEREST OF THE AMICUS CURAE

Peter Swire is now the J.Z. Liang Chair in the Georgia Tech School of Cybersecurity and Privacy. From 1999 to 2001 he served as Chief Counselor for Privacy in the U.S. Office of Management and Budget, the first person to have government-wide responsibility for privacy policy. In 2013, after the Snowden revelations, President Obama named him to serve as one of five members of the President's Review Group on Intelligence and Communications Technology, to recommend how to uphold both national security and liberty in U.S. intelligence programs. Swire has written extensively on foreign intelligence surveillance. Among his other activities, he has testified twenty-two times before the Congress, at the request of both parties. His interest in the case is to uphold the intricate statutory balance between national security and privacy / civil liberties that has been a principal focus of his career.¹

INTRODUCTION AND SUMMARY OF ARGUMENT

The Privacy and Civil Liberties Oversight Board (PCLOB), whose independence under its statute is at issue in this case, plays a unique role in responding to the history of constitutional and other legal violations under secret

¹ All parties have consented in writing to the filing of this brief. No entity or person aside from amicus curiae made any monetary contribution supporting the preparation or submission of this brief. No counsel for any party to this proceeding authored this brief in whole or in part.

U.S. government surveillance programs. Statutes governing secret government surveillance have drawn upon the Article I power of Congress and the Article III power of the courts, as well as the President's Article II authority, to address the unique features of secret surveillance. Even with a presumption that the President has the power to remove government officials without cause, the 2007 PCLOB statute was drafted precisely to enable independence and allow removal only for cause. The PCLOB's unique role also fits within the for-cause removal exception, because it stands in judgment of the Executive Branch, finding classified facts otherwise not obtainable, and rendering legal opinions.

Under the Fourth Amendment, foreign intelligence surveillance is judged under the "totality of the circumstances" reasonableness test. Rapid changes in technology and surveillance targets are common, calling for the continual oversight provided by the PCLOB. These constitutional requirements reinforce the argument that the structure and function of the PCLOB calls for independent oversight of secret government surveillance. The importance of PCLOB independence is reinforced by the longstanding U.S. government position that the Board is indeed independent, as shown for instance in diplomatic negotiations with the European Union to sustain trillions of dollars of annual U.S. trade.

ARGUMENT

I. The PCLOB is a Unique Agency to Address the Fundamental Constitutional Tension Between Liberty and Security

The Privacy and Civil Liberties Oversight Board (“PCLOB”), whose independence under its statute is at issue in this case, addresses the need both to protect national security and to ensure liberty. Secret government surveillance is essential in some settings, but also potentially and historically a severe threat to individual liberty and the preservation of the rule of law.

A. The PCLOB Plays a Unique Role in Responding to the History of Constitutional Violations Under Secret U.S. Government Surveillance Programs

The unique role of the PCLOB is that it responds to the history of secret U.S. government surveillance, with important infringements historically on both the First and Fourth Amendments. In the period before Watergate, the extent of secret surveillance was so great as to earn the title “The Lawless State” from one important study.² Martin Luther King, Jr. was the target of years of surveillance, as was protected expression by an enormous array of other actors. In the wake of Watergate, the famous Church Committee Report³ explained the challenge:

² See Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1316 (2004) (citing MORTON H. HALPERIN ET AL., *THE LAWLESS STATE: THE CRIMES OF THE U.S. INTELLIGENCE AGENCIES* (1976)).

³ *Final Report of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*. S. Rep. No. 755, 94th Cong., 2d Sess. (April 29, 1976) (“Church Committee Report”).

“[T]oo often ... intelligence activities have invaded individual privacy and violated the rights of lawful assembly and political expression.” This danger, the Committee observed, is inherent in the very essence of government intelligence programs, because the “natural tendency of Government is toward abuse of power” and because “men entrusted with power, even those aware of its dangers, tend, particularly when pressured, to slight liberty.” Moreover, because abuse thrives on secrecy, there is a natural “tendency of intelligence activities to expand beyond their initial scope” and to “generate ever-increasing demands for new data.”⁴

In a 2004 study of the history of secret U.S. surveillance, the amicus identified nine themes from the history: (1) routine violations of law; (2) expansion of surveillance for prevention and other purposes; (3) secrecy; (4) use against political opponents; (5) targeting and disruption of unpopular groups; (6) chilling of First Amendment rights; (7) harm to individuals; (8) distortion of data to influence government policy and public perceptions; and (9) cost and ineffectiveness.⁵ Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1316 (2004) (explaining the history).

Additional legal violations, and responses later from the PCLOB, occurred as

⁴ *Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies*, Liberty and Security in a Changing World, 58-59 (2013) (quoting Church Committee Report at v, vii, 1, 3).

⁵ The 1977 book entitled *The Lawless State: The Crimes of the U.S. Intelligence Agencies* devotes an annotated chapter to the history of illegal surveillance activities of several U.S. agencies-the FBI, the CIA, the Army, the IRS, and others. Those statistics, which provided a flavor for the scale of domestic surveillance, are the source material from which I identified my themes that show the important concerns raised by improper surveillance. See Morton H. Halperin et al., *THE LAWLESS STATE: THE CRIMES OF THE U.S. INTELLIGENCE AGENCIES* (1976).

part of the increase in secret surveillance after the attacks of September 11, 2001. As initially revealed in 2013 by the illegal leaks of Edward Snowden, the “Section 215” program, explicitly authorized for *foreign* intelligence surveillance, became the basis for collection of the *domestic* phone records of a large fraction of all Americans. A PCLOB report found the Section 215 program unlawful,⁶ and Congress in 2015 legislation ended the broad Section 215 authority. In addition, the program under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), discussed further below, had expanded far beyond what was known to Congress and the public, including with “incidental collection”⁷ of the communications of numerous Americans. After the PCLOB issued its report on Section 702 in 2014, that law was significantly amended.⁸ Subsequent PCLOB oversight of the Section 702 program, as discussed below, has resulted in multiple subsequent actions by Congress.

⁶ See PCLOB, *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*, at 104 (Jan. 23, 2014)

https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf.

⁷ Incidental collection” is collection that “occurs when a properly targeted non-U.S. person located abroad communicates with a U.S. person.” PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, at 97 (Sept. 28, 2023)

[https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20\(002\).pdf](https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20(002).pdf).

⁸ See PCLOB, *Recommendations Assessment Report*, at 3-15 (Jan. 29, 2015)

https://documents.pclob.gov/prod/Documents/OversightReport/a97a9918-775d-42eb-b426-2ae01838c2a3/Recommendations_Assessment-Report_2015%20-%20Complete%20-%20Nov%202%202022%201544.pdf.

PCLOB reports have also been relied upon by U.S. courts when finding violations of law. *See, e.g., United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019); *United States v. Muhtorov*, 20 F.4th 558 (10th Cir. 2021); *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016).

These important PCLOB actions in 2013 and afterwards occurred simultaneously with the amicus' role as one of five members of the President's Review Group on Intelligence and Communications Technology ("NSA Review Group"). The NSA Review Group was appointed in August, 2013 and published its report of over 300 pages that December.⁹ One reason for having both the PCLOB and the NSA Review Group conduct their reviews was that the PCLOB had lacked a Chair from the time of its second statute, in 2007, until May, 2013.¹⁰ There thus had not been ongoing PCLOB oversight and recommendations to Congress in the intervening period. In the absence of a functioning PCLOB, secret surveillance

⁹ *See Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, Liberty and Security in a Changing World, 58-59 (2013) ("NSA Review Group Report") The other members of the NSA Review Group Richard Clarke, senior advisor to Presidents Clinton and Bush on cybersecurity, Michael Morrell, former acting Director of the Central Intelligence Agency, and law professors Geoffrey Stone and Cass Sunstein. The NSA Review Group's office was shared with the PCLOB, although our work was done independently.

¹⁰ *See* Fabiola Carrion, *Cautious Optimism as US Privacy Oversight Board Finally Confirms Chair*, ACCESS NOW (Jan. 12, 2023), <https://www.accessnow.org/cautious-optimism-as-us-privacy-oversight-board-finally-confirms-chair>.

expanded dramatically. Agreeing with recommendations of the PCLOB¹¹ and the NSA Review Group,¹² Congress on a bipartisan basis enacted sweeping reforms in the USA FREEDOM Act of 2015. *See* Pub. L. No. 114-23, H.R. 2048, 114th Cong. (2015).

B. The Independence of the PCLOB is Clearly Established by the History of its Founding Statute

The history of secret national security surveillance, and legislative responses to that history, clearly establish that the PCLOB is a unique and independent agency, whose members can only be removed for cause.

After Watergate, Congress enacted FISA, which remains the charter for secret government surveillance for national security purposes. Although the President generally has broad authority over foreign affairs and national security under Article II of the Constitution, the FISA legislation drew upon the powers of all three branches of government to address surveillance directed at “foreign powers” yet

¹¹ *See* PCLOB, *Recommendations Assessment Report*, at 1 (Feb. 5, 2016), https://documents.pclob.gov/prod/Documents/OversightReport/8ab510df-738f-44b5-a73a-08d1336d544d/Recommendations_Assessment_Report_20160205%20-%20Completed%20508%20-%2010252022.pdf#:~:text=Consistent%20with%20PCLOB's%20recommendation%20C%20the%20USA%20FREEDOM,for%20appellate%20review%20of%20FISA%20court%20decisions.

¹² *See* Peter Swire, *The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years*, IAPP, (Jun. 8, 2015), <https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years/>.

conducted within the United States, where constitutional protections apply under the First and Fourth Amendments. FISA creates the Foreign Intelligence Surveillance Court (“FISC”) as a parallel judicial system for assessing foreign intelligence surveillance. FISA provisions create a complex and unique regime, with different rules for instance based on place of collection, identity of the target, and type of communication. Enacted in the wake of Watergate, FISA was designed to set binding limits on the President’s authority, while enabling national security surveillance that meets legal standards.

Congress has iteratively revised FISA and associate statutes over the years, as an intricate scheme for authorizing and regulating foreign intelligence surveillance. As part of that long arc of tinkering, Congress created the PCLOB and clearly gave it independence in 2007, for the reasons the parties’ briefs cover and the District Court found. I concur with the position of Appellees that the statutes clearly indicate that the members of the PCLOB are designed by statute to be removable only for cause. I briefly note the following. Acting on the recommendation of the 9/11 Commission, Congress passed legislation establishing the PCLOB, and President George W. Bush signed the law in 2004. Brief for Appellees at 28. One member of the Board, Lanny Davis, resigned after publicly objecting to the actions by the White House to line-edit a report by the PCLOB. *Id.* at 5. In response, Congress then enacted the second version of the PCLOB, which created the PCLOB as an

independent agency and, among multiple changes, notably removed language stating that the Board members “serve at the pleasure of the President.” *Id.*

II. The History of PCLOB’s Statute is Legally Relevant in Determining its Independence

This history is important in at least two ways to determining whether the PCLOB statute provides independence. First, even with a presumption that the President has the power to remove government officials without cause, the 2007 PCLOB statute was drafted precisely to enable independence and allow removal only for cause. The history shows that the statutes governing secret government surveillance have drawn upon the Article I power of Congress and the Article III power of the courts, as well as the President’s Article II authority, to address the unique features of secret surveillance, including the experience of unconstitutional executive expansions of surveillance activity conducted without the knowledge of Congress and the public.

Congress has carefully created an intricate statutory scheme to regulate, provide remedies for, and prophylactically address secret executive branch conduct, including through the PCLOB, the courts, and congressional oversight. Congress as an institution has a long-recognized ability to craft laws to remedy constitutional violations, most famously under the civil rights provisions of Section 1983.¹³ The

¹³ See, e.g., Jack Beerman, *A Critical Approach to Section 1983, With Special Attention to Sources of Law*, 42 STANF. L. REV. 51, 51 (1989) (“[T]he statute's

PCLOB's report on the Section 215 program found that the program violated the statute and quite possibly the Constitution, and Congress subsequently ended the program to avoid further violations.¹⁴ In addition, Congress similarly has the power to act prophylactically, to reduce the number and extent of constitutional violations.¹⁵ The creation of the PCLOB in the wake of the 9/11 Commission Report was itself prophylactic, responding to the concern about privacy and civil liberties violations in the wake of the changed law and facts after 9/11. Similarly, the second version of the PCLOB was prophylactic, based on the clear intent of Congress to provide more independent and effective oversight and legislative recommendations than existed under the prior statute. Therefore, even with a presumption that the President has the Article II power to remove government officials without cause, the history indicates vital Article I and Article III considerations, and so the presumption should not apply here.

Second, even if *Weiner v. U.S.*, 357 U.S. 349 (1958) is read as a narrow

broad language provides a remedy for violations of federal constitutional and statutory rights.”).

¹⁴ PCLOB, *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*, at 103-136 (Jan. 23, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf.

¹⁵ See, e.g., Calvin Massey, *Two Zones of Prophylaxis: The Scope of the Fourteenth Amendment Enforcement Power*, 76 GEO. WASH. L. REV. 1 (2007) (analyzing Congress' prophylactic power).

exception to the statutory presumption of presidential removal, the Appellees still win here. PCLOB has an adjudicative role with respect to national security surveillance – it stands in judgment of the Executive Branch, finding classified facts otherwise not obtainable,¹⁶ and rendering legal opinions. Although PCLOB is not literally a court, Article III courts have limited ability to reach these issues – intelligence wiretaps generally provide no notice to the target, a target does not learn about surveillance except in the rare instance where intelligence collection turns into a criminal trial, there often is no standing to challenge classified surveillance actions even if a person discovers they were a target, and the state secrets doctrine poses additional obstacles. In order to provide oversight comparable to the tribunal in *Wiener*, an independent PCLOB is uniquely required in order to provide transparency and make findings about needed changes to the law.

III. There is a Distinct Fourth Amendment Analysis for Secret Foreign Intelligence Surveillance, Supporting the Independence of the PCLOB

A. The PCLOB Oversees Reasonableness of the Fourth Amendment, But Not the Warrant Requirement

The application of the Fourth Amendment to secret foreign intelligence surveillance – a key focus of the PCLOB’s reports and recommendations – differs

¹⁶ As shown by its multiple, lengthy, expert reports, the PCLOB has a far greater ability to conduct detailed oversight of classified programs than the House and Senate intelligence committees.

from the familiar requirement of a probable cause warrant in the usual law enforcement proceeding. President Franklin Roosevelt, responding to the Second World War, was the first President to authorize wiretaps on national security grounds.¹⁷ In *Katz v. United States*, the Supreme Court held that a search warrant was required for a wiretap used for law enforcement purposes, but it declined to extend that holding to cases “involving the national security.” 389 U.S. 347, 358, n.23 (1967). The Supreme Court addressed the lawfulness of national security wiretaps in 1972 in *United States v. United States District Court*, 407 U.S. 297 (1972), often known as the “*Keith*” case. While requiring a search warrant requirement for domestic actions seeking to attack the government, the Court expressly reserved the issues of foreign intelligence surveillance: “[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country.” *Id.* at 308.

In 1978, Congress responded to *Keith* by enacting the Foreign Intelligence Surveillance Act,¹⁸ which, as amended, remains the basis for much of the foreign intelligence surveillance that exists today, and the focus of ongoing PCLOB

¹⁷ See Alison A. Bradley, *Extremism in the Defense of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT ACT*, 77 TUL. L. REV. 465, 468 (2002) (describing the limited nature of national security wiretaps authorized by President Roosevelt).

¹⁸ See Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1312-1325 (offering a detailed discovery on this history).

oversight.¹⁹ There are multiple differences between FISA and ordinary criminal law, but the most relevant here is that a search is authorized under FISA based on probable cause that the target is an agent of a foreign power, rather than requiring probable cause of a crime. 50 U.S.C. § 1805(a)(2)(A).

The standard for FISA surveillance shows that this surveillance is not conducted under the probable cause warrant provision in the Fourth Amendment, but instead under the general requirement that any search or seizure meet the reasonableness standard. “The ultimate touchstone of the Fourth Amendment is reasonableness.” *Riley v. California*, 573 U.S. 373, 381 (2014) (citing *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). In deciding reasonableness under the Fourth Amendment, courts generally examine “the totality of the circumstances” and weigh “‘the promotion of legitimate governmental interests’ against ‘the degree to which [the search] intrudes upon an individual’s privacy.’” *Maryland v. King*, 569 U.S.

¹⁹ Notably, the PCLOB has issued two major reports on Section 702 of FISA, as well as other work on FISA topics. See PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, (Jul. 2, 2014), <https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%202014%202022%201548.pdf>; PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, (Sept. 28, 2023), <https://documents.pclob.gov/prod/Documents/OversightReport/d21d1c6b-6de3-4bc4-b018-6c9151a0497d/2023%20PCLOB%20702%20Report,%20508%20Completed,%20Dec%202024.pdf>.

435, 448 (2013) (alteration in original) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). In the FISA context, the Foreign Intelligence Surveillance Court of Review has agreed “it has long been recognized that some searches occur in the service of ‘special needs, beyond the normal need for law enforcement,’ and that, when it comes to intrusions of this kind, the warrant requirement is sometimes a poor proxy for the textual command of reasonableness.” *In re Certified Question of L.*, 858 F.3d 591, 605 (Foreign Int. Surv. Ct. Rev. 2016) (citing *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)).

B. Changes in Technology and Surveillance Targets are an Important Feature of Secret Government Surveillance

Change is a constant for electronic surveillance – people use new forms of technology, and those conducting surveillance have to target new access points for information and new priority threats to the national security. The PCLOB’s oversight duties are to “continually review” aspects of secret surveillance. 42 U.S.C. § 2000ee(d)(2), and such continual review is vital to ensuring the reasonableness of government searches for such surveillance.

The history of the FISA 702 program – the subject of two of the PCLOB’s major, impactful reports – illustrates the ongoing need to update surveillance safeguards. The NSA Review Group analyzed factual changes after the attacks of 9/11:

For the most part, signals intelligence during World War II and the Cold

War did not involve collection and use on the equipment and networks used by ordinary Americans. Signals intelligence today, by contrast, pervasively involves the communications devices, software, and networks that are also used by ordinary Americans and citizens of other countries.

NSA Review Group Report at 180-181 (2013). The NSA Review Group identified three key changes relevant to the FISA 702 program. First is the change of target for secret surveillance, “from nation-states to well-hidden terrorists.” *Id.* at 181. Instead of targeting communications in a Soviet embassy, for instance, agencies try to find terrorist targets who hide their communications in “the vast sea of other communications,” overwhelmingly used for non-terrorist purposes. *Id.* at 182. Second is the shift “from domestic to foreign” – that distinction disappears because “terrorists and their allies use the same Internet as ordinary Americans.” *Id.* at 182-83. Third, national security surveillance shifted “from wartime to continuous response to cyber and other threats.” *Id.* at 184. Terrorists and hackers can attack the nation at any moment, as shown on 9/11, so the government seeks continual monitoring and rapid response.

With this post-9/11 convergence of civilian communications and intelligence collection, the intelligence community sought new wiretap authorities, notably for what became the FISA 702 program. Before the Internet, U.S. government collection of individuals in foreign countries happened in or near those foreign countries. Peter Swire, *U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013*, at 12 (Dec. 18,

2015), <https://peterswire.net/wp-content/uploads/Schrems-White-Paper-12-18-2015.pdf>. By contrast, the Internet developed so that a large and unprecedented portion of foreign communications came through the U.S. internet backbone, and often with storage or wiretap access via a U.S. provider. *Id.* Historically, wiretaps conducted within the territorial United States needed an individualized law enforcement or FISA order signed by a judge. *Id.* at 8. Congress, in the 2008 legislation creating the FISA 702 program, decided instead to respond to the technological changes, and authorize non-individualized judicial review for communications, where the target was neither a U.S. person nor within the U.S. *See* Pub. L. No. 110-261, 122 Stat. 2436, 118th Cong. (2008) .

The FISA 702 program enabled far more collections within the U.S., without individualized judicial review. It also created a new mechanism for gathering many communications of ordinary Americans, the so-called incidental collection that has been the subject of extensive criticism²⁰ by the PCLOB²¹ and the Foreign

²⁰ “Even though FBI analysts and agents who solely work on non-foreign intelligence crimes are not *required* to conduct queries of databases containing Section 702 data, they are *permitted* to conduct such queries and many do conduct such queries. This is not clearly expressed in the FBI’s minimization procedures, and the minimization procedures should be modified to better reflect this actual practice.” PCLOB, *Recommendations Assessment Report*, 16 (Feb. 5, 2016), https://documents.pclob.gov/prod/Documents/OversightReport/8ab510df-738f-44b5-a73a-08d1336d544d/Recommendations_Assessment_Report_20160205%20-%20Completed%20508%20-%2010252022.pdf. In response, Congress codified new requirements in 2018 for the FBI to query communications of U.S. persons.

²¹ *See* PCLOB, *Report on the Surveillance Program Operated Pursuant to Section*

Intelligence Surveillance Court (FISC).²² In short, creation of the FISA 702 program is one example of how changing technology and national security threats lead to novel intelligence programs, with significant implications for the privacy and civil liberties of Americans.²³

C. Independence of the PCLOB Protects Fourth Amendment Reasonableness and is Constitutionally Relevant to this Case

In applying the totality of the circumstances test, courts must assess all of the relevant safeguards, so that searches are done only for legitimate government interests and do not unreasonably intrude upon an individual's privacy. *See, e.g., Illinois v. Gates*, 462 U.S. 213 (1983). For example, the FISC applied this test in 2018 in holding that “the FBI's querying procedures and minimization procedures are not consistent with the requirements of the Fourth Amendment.” *Redacted*, 402

702 of the Foreign Intelligence Surveillance Act (Jul. 2, 2014), <https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%2014%202022%201548.pdf>; PCLOB, *Recommendations Assessment Report* (Jan. 29, 2015), http://documents.pclob.gov/prod/Documents/OversightReport/a97a9918-775d-42eb-b426-2ae01838c2a3/Recommendations_Assessment-Report_2015%20-%20Complete%20-%20Nov%202%202022%201544.pdf.

²² *See* Peter Margulies, *Searching for Federal Judicial Power: Article III and the Foreign Intelligence Surveillance Court*, 85 GEO. WASH. L. REV. 800, 843 (2017), <https://core.ac.uk/download/pdf/212910171.pdf>.

²³ As another example, changing encryption and cloud computing practices since 2000 have greatly shifted how the government targets communications. *See* Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud*, 2 INT'L DATA PRIVACY L. 200 (2012).

F. Supp. 3d 45, 92 (Foreign Intel. Surv. Ct. 2018). In applying the totality of the circumstances test, “the FISC has assessed the reasonableness of the government’s procedures as a whole, rather than separately analyzing the reasonableness of discrete forms of action taken thereunder, such as querying.” *Id.* at 85.

The PCLOB, acting as an independent agency, materially assists the reasonableness of the government’s procedures as a whole in multiple ways, including: (1) producing reports to Congress and the public based on classified information; (2) testifying before Congress, including with minority views;²⁴ (3) making expert recommendations about additional safeguards, based on its review of classified information; and (4) noting to the Congress and the public when the Executive branch decides not to follow its recommendations. *See* 42 U.S.C. § 2000ee. In the absence of such safeguards, and given the history discussed above of covert expansion of secret surveillance, the overall Fourth Amendment protections concerning a surveillance program would more likely become unreasonable over time.

The safeguards provided by an independent PCLOB are thus constitutionally relevant to the totality of the circumstances test – the presence of PCLOB’s safeguards may lead a court to conclude that a search, seizure, or surveillance

²⁴ Because the statute specifically states that the PCLOB shall provide minority views, the statute expects at least one viewpoint that differs from the current Executive branch view.

program is overall “reasonable,” or the absence of PCLOB’s safeguards may lead to the conclusion that it is not reasonable. Changes in technology and surveillance targets are an important feature of secret government surveillance, so continual and timely review by an independent body, such as the PCLOB, is needed to meet the constitutional standard of reasonableness.

IV. The Independence of the PCLOB is a Vital Aspect of the Statutory Structure and Function of the PCLOB

This Brief concurs with the discussion of structure and function in the Brief for Appellees at 28-39. The discussion above about the ways that the PCLOB protects the Constitution overlaps with the structure and function analysis – Congress has been repeatedly aware of constitutional problems that can arise from secret surveillance, and Congress has the power both to remedy constitutional and other legal violations, and to issue prophylactic laws to do so.

This Brief adds further information about how Congress and the courts rely on the PCLOB’s independence as essential to its structure and function. It documents the longstanding and previously-unbroken U.S. government position that the PCLOB is independent. As a prominent example of that unbroken position, the brief explains judicial proceedings and U.S. diplomacy related to the legal assessment by the European Union (EU) of the adequacy of U.S. legal safeguards against secret surveillance.

A. Additional Points Supporting the View that Congress and the Courts Rely on PCLOB's Independence as Essential to its Structure and Function

This Brief notes two examples, not explained in the Brief for Appellees, that illustrate how Congress has relied on the PCLOB to consider and make important reforms to legislation. In doing so, the independence of the PCLOB has been important to Congress' ability to respond to the cycle of increased covert government surveillance, and subsequent legal reform, discussed above. PCLOB's statutory mandate to publicly report on surveillance programs also plays a critical role in equipping courts with declassified information necessary to evaluate constitutional challenges to government action.²⁵

First, Congress adopted recommendations of the PCLOB in the FISA Amendments Reauthorization Act of 2017. Pub. L. No. 115-118, § 201(a)(1)(A), 132 Stat. 3, 19, 115th Cong. (2018). As part of the reauthorization, Congress adopted recommendations from the 2014 PCLOB Report²⁶ that called for specific limitations

²⁵ The district court stated correctly: "Courts have routinely referenced and relied upon the PCLOB's public representations and conclusions in reviewing legal challenges to certain government surveillance programs." *LeBlanc v. U.S. Priv. & C.L. Oversight Bd.*, No. 25-cv-542, 2025 WL 1454010 at n.5 (D.D.C. May 21, 2025).

²⁶ PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 137 (Jul. 2, 2014), <https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%2014%202022%201548.pdf>

on FBI querying of Section 702 information. The new statute mandated that a court order be entered before the FBI can access data collected pursuant to a United States person query term unrelated to foreign intelligence information. *Id.* §101(f)(2)(A), at 4.

The most high-profile issue in the 2024 FISA Reauthorization was whether to follow the recommendation of a majority of the PCLOB to require an individual court order for FBI agents and intelligence analysts to query U.S. person identifiers in the Section 702 database.²⁷ This recommendation was strongly opposed by the Biden administration, illustrating the ability of the PCLOB to make independent recommendations. *Id.* On a dramatic and bipartisan tie vote in the House of Representatives, the motion to adopt that PCLOB recommendation failed. *Id.* As a result, the Section 702 program was reauthorized, but only for two years rather than the expected five years. *Id.* The short reauthorization exemplifies the attention given by Congress to PCLOB reports and recommendations, and the importance of PCLOB independence to the Board's structure and function.

B. The Longstanding and Previously-Unbroken U.S. Government Position is that the PCLOB is Independent

The longstanding position of the U.S. government, based on my research and

²⁷ Charley Savage and Luke Broadwater, *House Passes Two-Year Surveillance Law Extension Without Warrant Requirement*, N.Y. TIMES, Apr. 12, 2024, <https://www.nytimes.com/2024/04/12/us/politics/surveillance-bill-fisa.html>.

personal experience, has been that the PCLOB is independent and its members can only be removed for cause. My research has not found any official U.S. government position before 2025 stating the contrary.

Three items illustrate this point. First, Executive Order 13636, issued in 2013, instructed the Department of Homeland Security to “consult with the Privacy and Civil Liberties Oversight Board.” Exec. Order No. 13636, 78 Fed. Reg. 11739, 11740 (Feb. 12, 2013). That is, the President did not treat the PCLOB as subject to his direct control, but instead instructed consultation with the Board. *Id.* Second, in January, 2021 the Chair of the PCLOB, Adam Klein, announced his resignation, stating “Consistent with the Board’s statutory independence, no one associated with the transition or White House has ever suggested that I should resign.”²⁸ That is, this appointee of President Trump, having served under that President, took care to emphasize “the Board’s statutory independence.”²⁹ Third, in the 2022 executive order that established redress procedures for the U.S/EU Data Privacy Framework, the President twice “encouraged,” rather than required, the PCLOB to take certain actions. Exec. Order No. 14086, 87 Fed. Reg. 62283, 62288, 62293, §2(c)(v)(A) &

²⁸ PCLOB, Press Release, Statement by Chairman Adam I. Klein on Intent to Resign as Chairman of the Privacy and Civil Liberties Oversight Board (Jan. 25, 2021), [https://documents.pclob.gov/prod/Documents/EventsAndPress/27d46947-d630-4d9d-83df-](https://documents.pclob.gov/prod/Documents/EventsAndPress/27d46947-d630-4d9d-83df-109f567cc0b0/Chairman%20Intent%20to%20Resign%20Jan%2025_21.pdf)

[109f567cc0b0/Chairman%20Intent%20to%20Resign%20Jan%2025_21.pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/27d46947-d630-4d9d-83df-109f567cc0b0/Chairman%20Intent%20to%20Resign%20Jan%2025_21.pdf).

²⁹ *Id.*

§3(e)(i) (Oct. 7, 2022).

i. The U.S Government and European Legal Authorities Have Emphasized the Independence of the PCLOB

For approximately ten years,³⁰ the independence of the PCLOB – the removal of PCLOB members only for cause – has been repeatedly emphasized by the U.S. government and European legal authorities in the context of the high-stakes legal proceedings concerning the quality of U.S. legal protections for personal data, particularly U.S. safeguards against excessive surveillance by the U.S. government. This history supports the view that the U.S. government has emphasized the independence of the PCLOB, and that the PCLOB’s structure and function is to provide independent reports and advice on legislative changes.

In the EU, an adequacy decision provides a legal basis in the law for transfers of personal data from EU countries to the United States for commercial purposes.

³⁰ As background, EU analysis of U.S. safeguards against excessive surveillance by the U.S. government has occurred in two cases decided by the Court of Justice of the European Union (“CJEU”). In 2015, in the *Schrems I* case, the CJEU invalidated the 2000 EU/U.S. Safe Harbor Agreement, with the CJEU finding that the safeguards against excessive U.S. surveillance of Europeans were not “essentially equivalent” to the safeguards required by European Union law. Case C-362/14, *Maximillian Schrems v. Data Prot. Comm’r*, ECLI:EU:C:2015:650, ¶¶ 96-98 (Oct. 6, 2015) (“*Schrems I*”). The EU and U.S. then negotiated the 2016 Privacy Shield Agreement. In the 2020 *Schrems II* case, the CJEU invalidated the Privacy Shield, with findings including a lack of adequate independence in the “redress” procedures available for EU persons under U.S. law. Case C-311/18, *Data Prot. Comm’r v. Facebook Ireland Ltd. and Maximillian Schrems*, ECLI:EU:C:2020:559, ¶ 201 (Jul. 16, 2020) (“*Schrems II*”).

Citing the independence of the PCLOB, the European Commission found in 2023 that the U.S. provides “adequate” protection. Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection under the EU-US Data Privacy Framework, 2023 O.J (L 231) 118, 144, 166. In 2023, the U.S. Department of Justice, explained the importance of this legal decision:

The adequacy decision provides a basis in the law of the European Union for transfers of personal data from EU countries to the United States for commercial purposes. *This flow of data underpins the \$7 trillion-dollar U.S./EU economic relationship* and provides vital benefits to citizens and businesses on both sides of the Atlantic, enabling businesses of all sizes to compete in each other’s markets.

Press Release, U.S. Dep’t of Just., Justice Department Statement on the European Union’s Adoption of Trans-Atlantic Data Privacy Framework to Restore Trust and Stability to Transatlantic Data Flows, Reflecting the Strength of EU-U.S. Relationship (Jul. 10, 2023) (emphasis supplied).

The meaning of independence is highly similar under EU and U.S. law, focused on whether the office-holder can only be fired for cause.³¹ The independence of the PCLOB has been repeatedly cited by European legal authorities, including

³¹ For instance, the CJEU has held: “the independence requirement ... must necessarily be construed as covering the obligation to allow supervisory authorities to serve their full term of office and to have them vacate office before expiry of the full term only in accordance with the rules and safeguards established by the applicable legislation.” Case C-288/12, *Eur. Commission v. Hungary*, ECLI:EU:C:2014:237, ¶¶ 55-56 (Apr. 8, 2014).

formal opinions of the European Commission,³² and in the opinions of the EU privacy regulatory expert agencies.³³ The EU General Court (the court directly beneath the CJEU), in a decision this month,³⁴ extensively discussed the importance in general of “independence” of review for EU law, and specifically cited the PCLOB and its independence: “The PCLOB was created in the heart of the executive power, and was conceived, by its founding statute, as an independent agency whose mission consists of supervising, in an impartial manner, the work performed by the executive.”³⁵ *Latombe*, ECLI:EU:T:2025:831, ¶ 54. In finding the new U.S. Data Protection Review Court (“DPRC”) “adequate,” the General Court specifically cited

³² See Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207); Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection under the EU-US Data Privacy Framework, 2023 O.J. (L 231).

³³ See Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision*, WP 238 (Apr. 13, 2016); European Data Protection Board, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework* (Feb. 28, 2023).

³⁴ On September 3, 2025, the General Court of the European Union (the court directly beneath the CJEU), found that the Data Privacy Framework assured sufficient independence and affirmed the Commission’s judgment that U.S. surveillance safeguards are now “adequate.” Case T-533/32, *Philippe Latombe v. European Comm’n*, ECLI:EU:T:2025:831, ¶ 8 (Gen. Ct. Sept. 3, 2025).

³⁵ At the time of writing, the opinion is available in French but not English, and the text is the author’s translation of this statement: “le PCLOB ait été institué au sein du pouvoir exécutif, il a été conçu, par son statut fondateur, comme une agence indépendante dont la mission consiste à superviser, de manière impartiale, le travail mené par le pouvoir exécutif.” *Latombe*, ECLI:EU:T:2025:831, ¶ 54.

the fact that the PCLOB would do an independent annual review of the operation of the DPRC. *Id.*

During this decade-long history, the importance of agency independence – removal only for cause – has long been known to the U.S. government during its negotiations with the EU on the data privacy issues. For instance, in the last phases of negotiation of the Privacy Shield in 2016, Robert Litt, then General Counsel for the Office of the Director of National Intelligence, wrote a formal letter to the EU explaining the role of the PCLOB: “[t]he PCLOB is an independent agency in the Executive Branch,” and “[t]he Board has two fundamental responsibilities — oversight and advice. The PCLOB sets its own agenda and determines what oversight or advice activities it wishes to undertake.” Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1, 106. If the President could remove the PCLOB members, then obviously the Board could not “set its own agenda” or determine what oversight it wishes to undertake.

In short, the 2023 Department of Justice statement about the importance of the EU/U.S. Data Privacy Framework, and Mr. Litt’s detailed example of the U.S. government’s formal, diplomatic representations, further confirm that the structure and function of the PCLOB includes the independence of the PCLOB.

CONCLUSION

If this Court determines that it has jurisdiction to hear this appeal, the decision of the District Court should be affirmed.

Dated: September 12, 2025

/s/ Peter Swire

Professor Peter Swire

Counsel of Record

2026 Castleway Lane NE

Atlanta, GA 30345

(240) 994-4142

peter@peterswire.net

CERTIFICATE OF COMPLIANCE

This brief complies with the type volume limitations of Federal Rules of Appellate Procedure 29(a)(5) and 32(a)(7)(B) because it contains 6299 words, excluding the parts exempted by Rule 32(f).

This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a) and the type style requirements of Rule 32(a)(6) because it appears in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman Font.

Dated: September 12, 2025

/s/ Peter Swire

Professor Peter Swire
Counsel of Record
2026 Castleway Lane NE
Atlanta, GA 30345
(240) 994-4142
peter@peterswire.net

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system on September 12, 2025, and the text of the electronic brief is identical to the text of the paper copies.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: September 12, 2025

/s/ Peter Swire

Professor Peter Swire
Counsel of Record
2026 Castleway Lane NE
Atlanta, GA 30345
(240) 994-4142
peter@peterswire.net