Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Atlantic Council
EUROPE CENTER

ISSUE BRIEF

Avoiding the Next Transatlantic Security Crisis: The Looming Clash over Passenger Name Record Data

JULY 2021 KENNETH PROPP

With transatlantic air travel poised to recover from the COVID-19 pandemic, a linchpin aviation security agreement between the United States and the European Union on passenger name record data is under threat in Brussels and in need of senior-level attention from policy makers.

Following the demise of the Privacy Shield Framework in the Schrems II judgment[1] at the Court of Justice of the European Union (CJEU) in the summer of 2020, the Joseph R. Biden, Jr. administration and the European Commission renewed a consequential negotiation to reestablish stable ground rules for the transfers of personal data that are built into the transatlantic economy.[2] The problem has the attention of US Cabinet secretaries and European commissioners, and has prompted urgent corporate appeals for a solution. Separately, Washington for now quietly continues to receive airline passenger information under a 2012 international agreement with Brussels that a recent European Parliament resolution criticizes as failing to meet the CJEU's strict data protection standards.[3] To avoid another transatlantic data transfer crisis—one that would have major consequences for airline security—the Biden administration needs to devote senior-level attention to the US-EU Passenger Name Record Agreement and to re-engage with the European Union on its future.

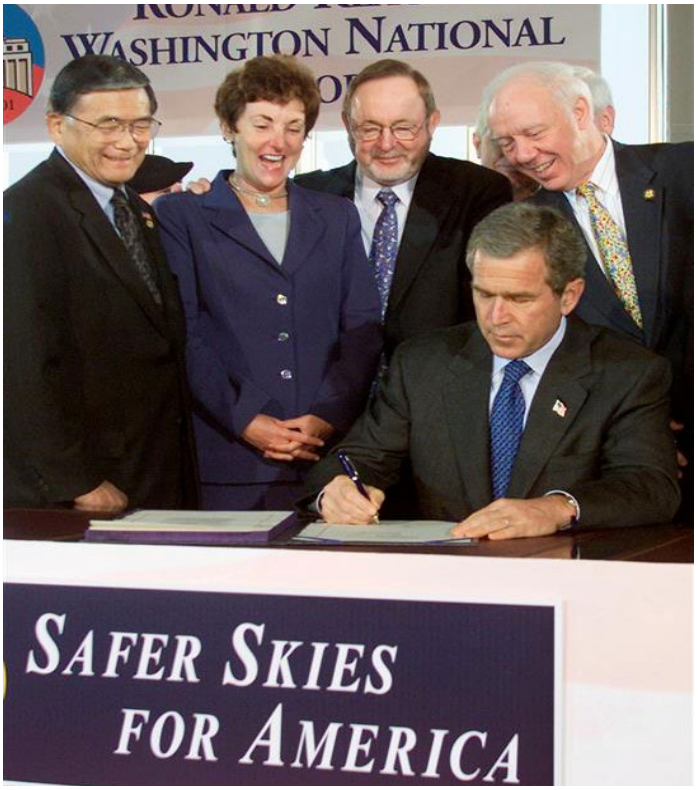
Background

The September 11, 2001, attacks on the United States awakened the country to the threat from foreign Islamist terrorist groups, and quickly led to a series

1 Case C-311/18, *Data Protection Commissioner v. Maximillian Schrems,* EU:C:2020:559. The judgment is known as *Schrems II* because it is the second case to be decided by the CJEU brought by the Austrian privacy activist challenging Facebook's commercial data transfers to the United States.

2 See, e.g., Kenneth Propp, "Return of the Transatlantic Privacy War," *New Atlanticist*, Atlantic Council, July 20, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/return-of-the-transatlantic-privacy-war/.

3 The resolution calls upon the commission to present the Parliament's Committee on Civil Liberties, Justice and Home Affairs by September 30, 2021, with a written analysis of how it intends to bring the agreement into line with the court's jurisprudence. European Parliament resolution of May 20, 2021, para. 25. European Parliament, "Texts Adopted - Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems ('Schrems II') - Case C-311/18," May 20, 2021, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html.



Then-President George W. Bush signs the Aviation and Transportation Security Act, allowing law enforcement to collect PNR data on all international flights to and from the United States. REUTERS/Larry Downing.

of dramatic changes in US government security policies. Expert inquiries, including the 9/11 Commission, identified weaknesses in US security and changes needed to secure civil aviation. The Department of Homeland Security (DHS) was established, the Aviation and Transportation Security Act (ATSA)[4] was enacted, and law enforcement and national security agencies began to exercise sweeping new powers to collect information to guard against future terrorist incidents on the scale of 9/11.

One component of ATSA, relatively unnoticed initially, required airlines systematically to provide passenger name record (PNR) data on all international flights to and from the United States to Customs and Border Protection (CBP), which would become a component of the new DHS.[5] PNR data consist of the information an individual provides to an airline electronic reservation system, including address, telephone and credit card numbers, and potentially sensitive information such as meal preferences or special needs that may indicate ethnic origin or religious belief. CBP reviews these data before an international flight departs to screen for connections among passengers and any known or suspected terrorists or criminals. Its assessment can lead to questioning before boarding or denial of permission to travel.

Although systematic information on how PNR data have foiled terrorist attacks or aided criminal investigations is not available, DHS occasionally discloses particulars. Three notorious cases over 2009-2011 illustrate the power of PNR data to disrupt terrorist plots. In one case, Faisal Shahzad attempted to set off an explosive in an automobile in Times Square, New York City.[6] His efforts to disguise his identity included purchasing the car for cash, not identifying himself to the seller, and failing to register the vehicle. His identity was revealed to authorities, however, when the cell phone number he gave to the seller matched a number of a connection to Pakistan in a database derived from PNR data on a flight Shahzad had taken years earlier. After evading Federal Bureau of Investigation (FBI) surveillance following the failed bombing, Shahzad made a flight reservation to the United Arab Emirates and drove to John F. Kennedy Airport. When the airline reported his PNR data to DHS, it immediately set off an alarm. A CBP officer removed him from the airplane.

In another case, PNR data provided crucial information to identify US citizen David Headley as the plotter of a planned terrorist attack in Europe. Based on a tip from an allied security service that knew only his first name, a travel routing, and a general time period for travel, CBP was able within hours to use PNR data to provide the FBI with his full name, address, passport number, and other information that led to his arrest. After Headley's arrest, it was found that he was also connected to the November 2008 Mumbai terrorist attack that killed 166 people, including six Americans.[7] It was also determined that he was plotting a second terrorist attack in Europe, targeting cartoonists at a

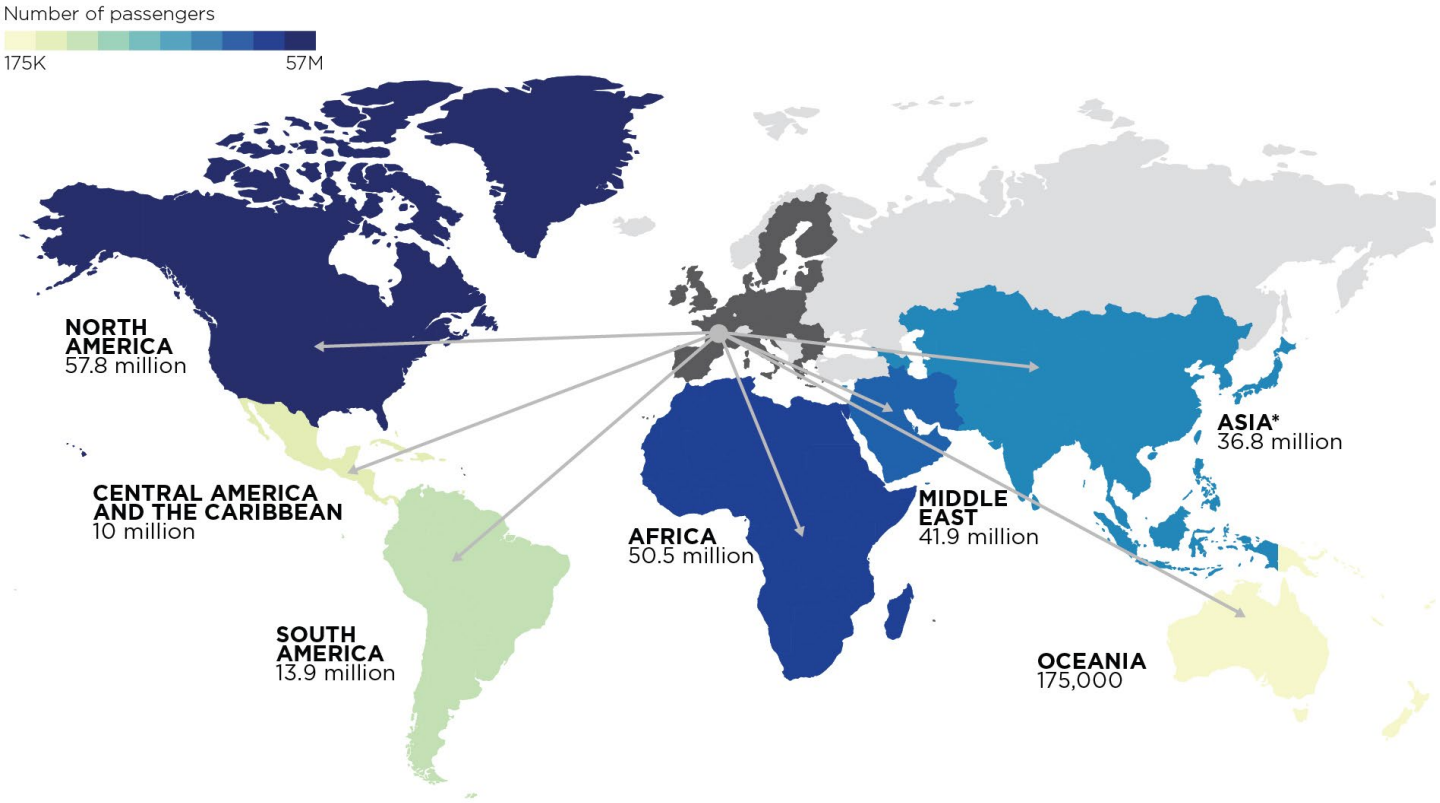
4 USA Patriot Act, Public Law 107-56, 115 Stat. 272, October 26, 2001.

5 Ibid., codified at 49 U.S. Code § 44909. Implementing regulations are found at 19 Code of Federal Regulations § 122.49d.

6 "Faisal Shahzad Indicted for Attempted Car Bombing in Times Square," US Department of Justice, Office of Public Affairs, June 17, 2010.

7 Tom Jennings, "David Coleman Headley: The Perfect Terrorist?" PBS *Frontline,* May 22, 2011, https://www.pbs.org/wgbh/frontline/article/david-coleman-headley-the-perfe/.

Passenger Air Travel through and from EU Member States to Non-European Regions, 2019



Source: Eurostat - International extra-EU air passenger transport by reporting country and partner world regions and countries. Data reflects each country's own reporting.

*Asia includes the Far East, Indian Subcontinent, and Asian Republics of the ex-USSR, as defined by the EU.

Danish newspaper. He was sentenced to thirty-five years in prison for these crimes.[8]

In a third case, PNR data led to the identification and arrest of two associates of Najibullah Zazi in a 2009 plot to set off bombs in the New York City subway system. In 2008, CBP records showed that Zazi and several associates flew from Newark to Peshawar, Pakistan, where some of them, including Zazi, received training from al-Qaeda. It was PNR data that connected Zazi and two of his associates—Adis Medunjanin and Zarein Ahmedzay. Ultimately, all three were arrested for a plot in August-September 2009 to use explosives in backpacks in a suicide attack.

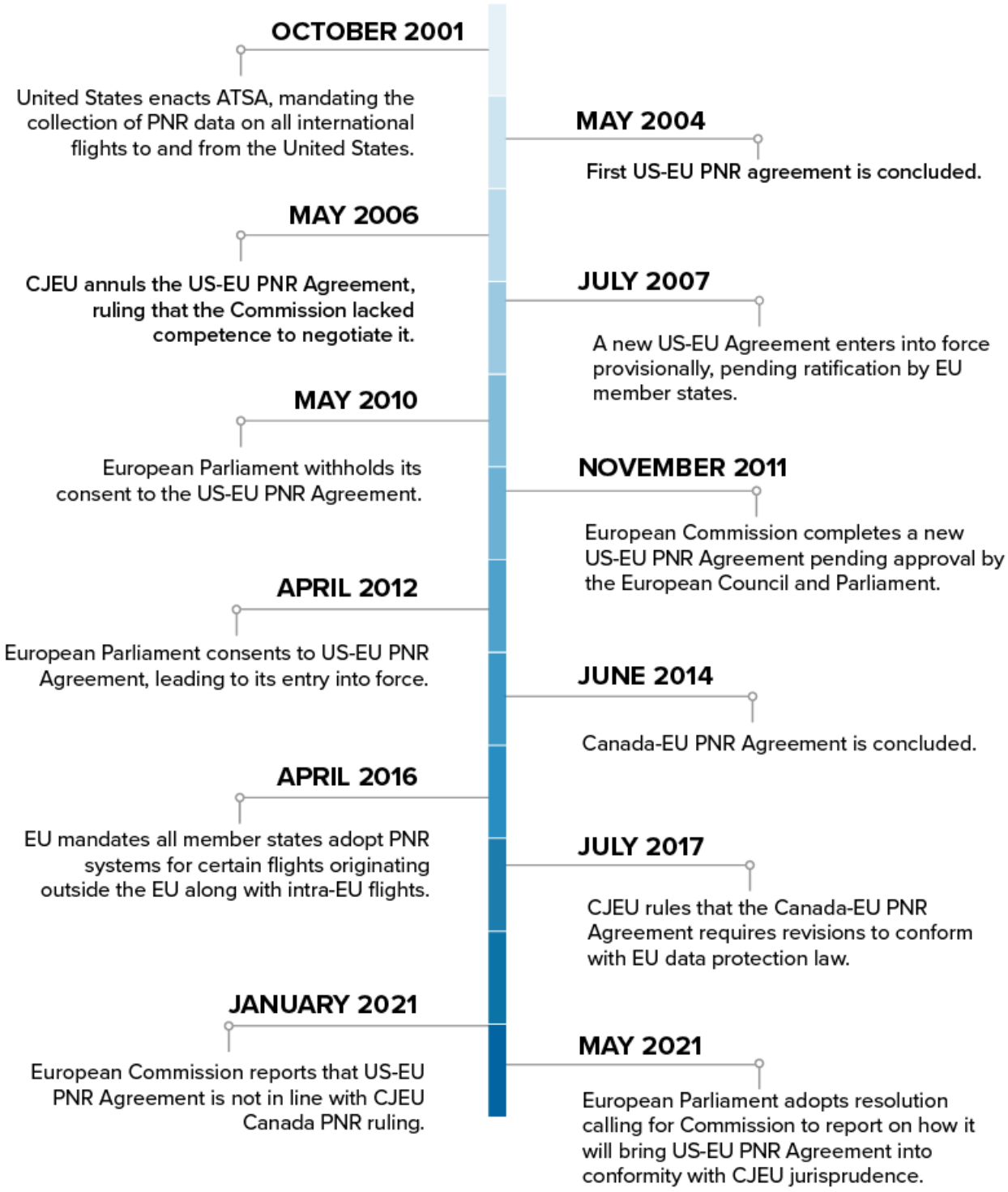
While the United States led the way internationally in making PNR data a central element of its counterterrorism and border security strategies, today there is general agreement about the data's value in making it harder for terrorists and criminals to fly internationally, and easier to detect them when they do. In 2016, in the wake of devastating terrorist attacks in Paris and Brussels, the EU mandated that its member states adopt their own PNR systems for many flights originating outside the EU as well as for intra-EU flights.[9]

As a result, member states increasingly have developed their own PNR analytical capacities. They have reported

8 US Department of Justice, "David Coleman Headley Sentenced to 35 Years in Prison for Role in India and Denmark Terror Plots," press release, January 24, 2013, https://www.justice.gov/opa/pr/david-coleman-headley-sentenced-35-years-prison-role-india-and-denmark-terror-plots.

9 European Parliament, *Directive (EU) 2016/681 of the European Parliament and of the Council on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation, and Prosecution of Terrorist Offences and Serious Crime, 2016 O.J. L 119, p. 133.*

TIMELINE OF KEY TRANSATLANTIC PNR DEVELOPMENTS



Source: European Parliament and European Commission compiled by the Atlantic Council.

Then-US Homeland Security Secretary Janet Napolitano holds a news conference following the arrest of Faisal Shahzad. Authorities used PNR data to arrest him when he attempted to flee to Dubai. REUTERS/Kevin Lamarque.

measurable success in using their harmonized PNR systems to identify terrorist suspects and persons involved in other serious crimes, including enabling arrests of persons previously unknown to the police.[10] They particularly value the retention of historical PNR data on such suspects for five years, so that "it is possible to review the travel history and see who travelled with him or her, identifying potential accomplices or other members of a criminal group, as well as potential victims," according to a European Commission report on member state PNR systems.[11] Member states see PNR data as a unique tool for this purpose, according to the report. Member state authorities regularly cooperate with CBP, and in turn receive relevant CBP PNR analysis.

Efforts to broaden PNR analysis and sharing globally have also advanced at the United Nations (UN), with European support. In 2017, UN Security Council Resolution 2396, adopted on a unanimous basis, established a requirement that all states develop and use PNR systems.[12] This mandate led to work at the International Civil Aviation Organization (ICAO) that resulted in new PNR standards and recommended practices three years later.[13] One provision of the standards anticipates international sharing of PNR data among ICAO members and prohibits penalizing airlines that transfer PNR data compliant with ICAO standards.[14] Others recommend retaining PNR information, including depersonalized data, and allowing for additional arrangements to promote collective security.

After September 11, 2001, airlines flying from Europe to the United States welcomed PNR screening but also realized that complying with the US legal requirement could put them in violation of European data protection law.[15] Under this body of EU law, personal data may leave EU territory only if they satisfy an authorized basis for data transfer. Since the EU did not accept the initial US view that purchase of an airplane ticket conferred a passenger's implicit consent to transfer his or her PNR data to the US government, the solution was for the European Union and the United States to negotiate an international agreement under which the EU itself would consent to the transfer of European-origin PNR information from its territory.[16] In return, the United

10 European Commission, *Report from the Commission to the European Parliament and the Council on the Review of Directive 2016/681 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime*, 305 final, July 24, 2020.

11 Ibid., 8.

12 United Nations Security Council Resolution 2396 (2017), operative paragraph 12.

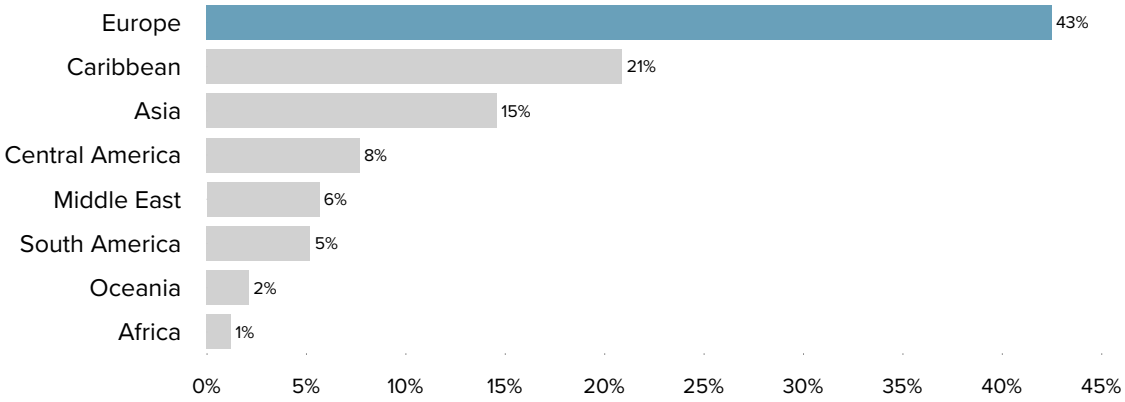
13 International Civil Aviation Organization, *PNR Standards and Recommended Practices*, June 2020, Working Paper FALP/11-WP/2, Annex 9 (Facilitation), Chapter 9, Section D.

14 Ibid., Standard 9.34(a). The EU filed a formal difference with this provision noting that EU member states are obliged to impose stricter requirements in PNR transfer arrangements with other ICAO members due to EU privacy law. European Commission, *Council Decision on the Position to Be Taken on Behalf of the European Union as Regards Annex 9 to the Convention on International Civil Aviation*, 5386/21, January 26, 2021.

15 European Parliament, Council of the European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, O.J. L 281, 23.11.1995, p. 31 (no longer in force). The General Data Protection Regulation (GDPR) replaced this measure and took effect in 2018. O.J. L 119/1, 4.5.2016, p. 1.

16 The question of whether personal data could be transferred under EU law is separate from whether the United States could impose the requirement that international passengers arriving in its territory could be required to provide their PNR data. The latter is authorized under Article 13 of the Convention on International Civil Aviation, December 7, 1944 (Chicago Convention), https://www.icao.int/publications/Documents/7300_orig.pdf. This provision of the Chicago Convention provides the international legal basis for the United States and other states party to require airlines to provide PNR data when entering, departing, or overflying their territories.

US Citizen Overseas Air Travel by Region, 2019



Source: International Air Travel Statistics Program (I-92, US International Trade Administration)

States government would provide privacy guarantees largely corresponding to EU privacy law.

Negotiation of this agreement proved no simple task. A first agreement was reached in 2004,[17] but the European Parliament contested the adequacy of the US privacy protections before the CJEU. The resulting 2006 judgment had the effect of annulling the agreement, although without reaching the merits, due to the court's finding that the commission lacked competence to negotiate. That judgment led to a hasty renegotiation.[18] The successor 2007 agreement itself succumbed several years later to political pressure from the European Parliament to strengthen the agreement's privacy provisions, and a new agreement was negotiated in 2011 and entered into force the following year.[19]

Under the 2012 agreement, the United States agreed to utilize EU-origin airline passenger data only for the prevention, detection, investigation, and prosecution of terrorist offenses or serious transnational crimes—not for any lesser criminal offense. CBP may also use PNR data at the border to determine whether to subject an individual to additional questions, known as secondary screening, and in individual cases of serious threat or for the protection of an individual's vital interests (such as the health of a traveler who may have been exposed to a contagious disease).

The 2012 agreement enables CBP to retain EU-origin PNR data in an active database for five years, and thereafter in a dormant database for ten years for use in transnational crime matters and for fifteen in terrorism matters. Except during an initial six-month period, such data must be stored in de-identified form, and may be re-personalized only in connection with a specific law enforcement operation. CBP also may utilize sensitive personal information contained in PNR data, such as that about meal selection or medical status, but must handle such data in more restricted ways.

Finally, the United States pledged to treat EU-origin PNR data in accordance with a set of data privacy and security rules closely based on EU law. For example, CBP must be transparent about its procedures, allow individuals access to their PNR data, and permit them the opportunity to correct erroneous data. EU citizens also have the important right to judicial review of US administrative decisions on handling of their PNR data. The scope of this right was significantly expanded by the subsequent 2016 US-EU Agreement on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and

17 *Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs*, 2004 O.J. L 183, May 20, 2004, p. 84 (no longer in force).

18 Joined Cases C-317 & 318/04, *European Parliament v. Council and Commission*, EU:C:2006:346.

19 *Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security*, 2012 O.J. L 215, p. 5.

Members of the European Parliament vote on the EU PNR Directive in 2016, obliging EU countries to collect PNR data. REUTERS/Vincent Kessler TPX IMAGES OF THE DAY.

Prosecution of Criminal Offences (also known as the Umbrella Agreement).[20]

US and EU governmental teams conduct periodic reviews of compliance with the agreement.

It has functioned reasonably smoothly over the past decade, as the most recent joint review attests.[21] Other countries saw the US agreement for obtaining access to EU-origin PNR data as a model and sought their own similar agreements. The EU has reached PNR agreements with Australia and Canada, and undertaken negotiations with Japan and Mexico.[22]

CJEU Jurisprudence

Despite the increased global acceptance of the value of PNR data collection, analysis, and sharing in recent years, some critics still claim that the loss of privacy, particularly when data are transferred internationally, outweighs security benefits. European data protection authorities and members of the European Parliament's Civil Liberties Committee consistently take this position, although EU member states, particularly those with longer experience in using PNR information for security purposes, and the commission itself tend to view PNR data in a more favorable light.

In 2015, the European Parliament sought the opinion of the CJEU on whether the Canada-EU PNR Agreement negotiated by the commission conformed to the provisions of the Charter of Fundamental Rights relating to data protection. Two years later, the court ruled that the draft Canada agreement was incompatible with EU law in a number of respects. While the CJEU opinion[23] found that international transfers of personal data for counter-crime purposes in principle were permissible under the charter, it nevertheless determined that a series of provisions of the Canada agreement failed the strict necessity and proportionality test applied to infringements of the fundamental right to data protection under European law. It held that certain categories of Europeans' PNR data were too sensitive to be transferred at all,[24] while other categories of data eligible for transfer were too broadly defined.[25] The court also exercised its extraterritorial jurisdiction over EU-origin personal data to insist that Canada conduct judicial or administrative review prior to using transferred PNR data

A statue of Lady Justice stands outside the EU Commission during a protest. REUTERS/Francois Lenoir.

20 *Agreement on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses* 2016 O.J. L 336, p. 3. Article 19 required the United States to amend its Privacy Act, which previously had limited such redress to US citizens.

21 European Commission, *Report from the Commission to the European Parliament and the Council on the Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Records to the United States Department of Homeland Security*, January 19, 2017, COM (2017) 29.

22 Since Brexit, exchange of PNR data among EU member states and institutions and the United Kingdom has been governed by the Trade and Cooperation Agreement between the European Union and the United Kingdom, 2020 O.J. L 444, p. 14, Part Three, Title III. Its terms essentially mirror the EU PNR Directive, which previously applied to the United Kingdom as an EU member state.

23 Opinion 1/15, *Draft Agreement between Canada and the European Union on Transfer of Passenger Name Record Data, Opinion of the Court (Grand Chamber),* EU:C:2017:592.

24 Ibid., paragraph 165.

25 Ibid., paragraphs 156-157, paragraph 160.

KEY DIFFERENCES BETWEEN US-EU PNR AGREEMENT AND CJEU JURISPRUDENCE

2012 US-EU PNR AGREEMENT	2017 CJEU CANADA-EU PNR JURISPRUDENCE
Allows US to utilize EU-origin PNR for crime prevention, detection investigation, and prosecution of terrorist offenses or serious transnational crime.	Insists Canada conduct judicial or administrative review prior to using transferred PNR data for purposes other than border control.
Allows US to retain EU-origin PNR data in an active database for five years, and in a dormant database for 10 years for use in transnational crime matters, and for 15 in terrorism matters.	Requires PNR be deleted immediately after travel, except on persons who already have been identified as presenting a terrorism or other serious criminal risk.
Grants CBP usage of sensitive PNR data such as information about meal selection or medical status in restricted ways.	Rules certain categories of PNR too sensitive to be transferred at all, while other data eligible for transfer were too broadly defined.
US pledges to treat EU-origin PNR in accordance with data privacy and security rules based on EU law.	Scope of data transfer under agreement fails the strict necessity and proportionality test applied to infringements of the EU fundamental right to data protection.

for purposes other than border control,[26] impose additional controls on onward disclosure to third countries,[27] and identify an internal oversight authority with greater independence.[28]

The commission's latest internal report expresses the view that the US-EU PNR Agreement, concluded before the *Canada PNR* opinion, is "not fully in line" with the court ruling.[29] Topics addressed in the US-EU agreement

26 Ibid., paragraphs 208-209.

27 Ibid., paragraph 215.

28 Ibid., paragraph 232.

29 European Commission, *Report from the Commission to the European Parliament and the Council on the Joint Evaluation of the Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security*, January 12, 2021, COM (2021) 18.

Canadian President Justin Trudeau and European Council President Charles Michel hold a news conference during the 2021 EU-Canada Summit. The EU and Canada are still negotiating a PNR agreement. REUTERS/Yves Herman.

and cited by the commission as problematic include "the retention of PNR data, the processing of sensitive data, notification to passengers, prior independent review of the use of PNR data, rules for domestic sharing and onward transfers, [and] independency of oversight…"[30]

Some of these differences are significant from a security perspective. For example, the United States fought hard in the 2012 negotiation for the ability to utilize, subject to safeguards, sensitive PNR data that would suggest a traveler's religion, such as in-flight meals, because of its potentially important predictive counterterrorism value, whereas the CJEU absolutely precludes the transfer of such data outside EU territory. In addition, US negotiators saw potential investigative value in retaining PNR data on all travelers from Europe in a dormant database for a period of ten to fifteen years after travel. The CJEU by contrast requires that PNR data be deleted immediately after travel, except on persons who already have been identified as presenting a terrorism or other serious criminal risk, in which case five years' retention is deemed proportionate.

The disagreement between homeland security authorities, not just in the United States, and the CJEU over the duration of PNR data retention is at least in part philosophical. Law enforcement officials in many countries would agree with the US perspective that rapid deletion of PNR information "would defeat the whole point" of securing air travel since "sometimes it won't be clear that a given piece of information is valuable until years after the fact."[31] The European Commission and member states expressly argued to the CJEU that membership in terrorist and criminal networks sometimes reveals itself only after years, but the generalist court found such evidence unpersuasive. Rather, the CJEU chose to stress its concern that a foreign government would be retaining a body of detailed personal data on presumptively innocent EU persons for a decade or longer.

30 Ibid.

31 Remarks of Ambassador Nathan A. Sales, "Counterterrorism, Data Privacy, and the Transatlantic Alliance," Coordinator for Counterterrorism, US Department of State, German Marshall Fund, July 19, 2018.

The divergences from EU fundamental rights law highlighted in the *Canada PNR* opinion have not so far led the EU to terminate the agreement with the United States and to pursue a successor agreement. On the contrary, the commission has remained publicly supportive of the US-EU PNR Agreement, which has continued to operate without interruption.

Instead, the commission decided first to renegotiate its draft PNR agreement with Canada along the lines required by the CJEU before tackling the challenge of the United States. The *Canada PNR* opinion presented the European Commission with an extremely prescriptive and challenging roadmap for renegotiating its draft PNR agreement with Canada, however. The EU court, unlike the US Supreme Court, does not defer to its "executive" branch negotiators to broadly define the content of international agreements. The consequences of the commission's lack of negotiating discretion are evident: Four years later, it still has not achieved a signed text with Canada, although efforts to complete that agreement continue.

Policy Recommendations

Counterterrorism policy in the United States has traditionally been bipartisan. Indeed, while the Barack Obama administration made a number of changes to George W. Bush administration policies, it did not dismantle its predecessor's counterterrorism architecture, sometimes to Europe's surprise. The 2012 US-EU PNR Agreement, concluded and implemented during the Obama administration, was vigorously defended in turn by the Donald Trump administration.

French border police screen air passengers upon arrival in Nice as part of heighted COVID-19 measures. The pandemic has highlighted the importance of air travel data to track the spread of COVID-19. REUTERS/Eric Gaillard.

In 2017, Assistant to the President for Homeland Security and Counterterrorism Thomas Bossert, speaking at the UN Global Counterterrorism Forum, stressed that any change in transatlantic PNR transfers "would not be welcome."[32] In a 2018 speech, Ambassador Nathan A. Sales, then-Department of State coordinator for counterterrorism and previously a Department of Homeland Security senior official, likewise stated that "[T]he United States is not prepared to renegotiate our PNR agreement. We simply cannot accept any additional restrictions on our ability to use PNR beyond what we accepted in 2012."[33]

While the Biden administration has indicated it will prioritize improving relations with Europe, early signs, including the return of key Obama administration personnel, make it likely to continue to stress the importance of transatlantic transportation security.

Most recently, the COVID-19 pandemic that spread from China in late 2019 caused many governments to appreciate anew the importance of airline passenger information, especially PNR data. DHS's insistence to European counterparts during the negotiation of the 2012 PNR Agreement that a legitimate use of PNR data was for the protection of a traveler's vital interests was demonstrated early in the pandemic in 2020 when it became possible to use PNR data to trace passengers who had traveled to areas with early or higher-than-usual rates of infection, or who had sat next to other passengers later determined to have been infected by COVID-19. Senior officials of two Middle Eastern governments told Atlantic Council scholars in March 2020 that PNR data demonstrated their value because government security and public health ministries could determine which of their citizens had traveled to countries, like China or Iran, that were suspected of underreporting COVID-19 infections, especially in the pandemic's early weeks. PNR data were considered more reliable than self-reporting.[34]

Nonetheless, the durability of the current situation is not clear. The Islamic State of Iraq and al-Sham's (ISIS's) loss

32 Remarks of Thomas Bossert, Special Assistant to the President for Counterterrorism, Global Counterterrorism Forum, September 20, 2017. Department of State on Twitter: "Assistant to @POTUS Tom Bossert participates in the Global Counterterrorism Forum (#GCTF) Ministerial on the margins of #UNGA. #USAatUNGA," https://t.co/Hncj2jQjI0.

33 Sales, "Counterterrorism, Data Privacy, and the Transatlantic Alliance."

34 Field interviews in March 2020 by Atlantic Council experts.

President Biden joins Commission President Ursula von der Leyen and Council President Charles Michel at the 2021 US-EU Summit. Any future PNR agreement will require high-level support. REUTERS/Yves Herman.

of territorial control in Iraq and Syria and the sharp drop in international air travel due to COVID-19 have ironically served to submerge the PNR issue's profile. A new set of PNR-related judicial challenges, to the EU's own PNR law, are pending before the CJEU.[35] The commission must take account of CJEU jurisprudence. Last year the commission launched a consultative process with EU citizens and stakeholders to rethink its entire approach to international PNR data transfers.[36]

The commission's so-called Roadmap sketches several possible alternative approaches: a unilateral EU law on international transmission of PNR data reflecting both the ICAO standards and the EU's higher privacy standards, which non-EU member states would have to meet; a slimmed-down model EU bilateral arrangement linked to the ICAO standards, for use in negotiations with non-EU states; or a reorientation toward negotiating a multilateral PNR agreement among EU and non-EU states. The commission has not yet indicated when it will publish a definitive policy recommendation.

In all likelihood, future transfers of EU-origin PNR data to the United States will still require some form of bilateral agreement, probably linked in some fashion to ICAO's work. Both the United States and the European Union need a stable and durable agreement negotiated by subject-matter experts. The alternative would place airlines and passengers in the untenable position of being caught in a conflict between US PNR collection law and EU privacy law. Moreover, PNR collection and use is no longer just a US government interest. Now that EU member states operate their own PNR systems and benefit from PNR data originating from a variety of countries, they too need data to flow smoothly.

35 Case C-817/19, *Ligue des droits humains v Conseil des ministers*, filed October 31, 2019; see also Joined Cases C-148/20, C-149/20, and C-150/20, *Deutsche Lufthansa AG*, filed March 16, 2020. Both sets of cases question whether generalized retention of PNR data on intra-EU flights pursuant to Directive 2016/681 is consistent with the data protection provision of the Charter of Fundamental Rights. Oral hearing has not yet occurred, and judgment is unlikely to be issued before the end of this year.

36 European Commission, "Roadmap: The External Dimension of the EU Policy on Passenger Name Records," July 24, 2020, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-.

The United States should take advantage of the interval afforded by the EU's ongoing internal reflection on international PNR data transfers to identify its own redlines as well as potential areas of transatlantic cooperation on PNR information. Two topics requiring particular attention are the duration of data retention and the utilization of "sensitive" data. In other areas, such as administrative oversight and prior independent authorization on the use of PNR data, the United States may be able to adapt existing domestic mechanisms—drawing upon the experience being gained in the ongoing US-EU commercial data privacy negotiations triggered by the *Schrems II* judgment.

The United States may benefit in a future negotiation from growing political discontent among EU member states over the expanding scope of data protection restrictions that the CJEU has placed on its own law enforcement and national security agencies regarding data retention. In a series of judgments beginning in 2014, the court struck down EU-level and member state laws allowing bulk retention of communications metadata for potential law enforcement access. In 2020, it went further, also placing restrictions on member state foreign intelligence collection that utilized private communications service providers.[37]

Recently, a number of EU member states, led by France, have rebelled against the CJEU's imposition of these data protection restrictions on their national security activities, an area that the EU's foundational Treaty on European Union declares as "the sole responsibility of each Member State."[38] France proposed that the pending ePrivacy Regulation be amended to categorically place all national security data collection activities outside the scope of EU law.[39] Separately, it asked its highest national administrative court, the Conseil d'Etat, to rule that the CJEU had acted beyond its scope in the 2020 judgments.[40] The French court declined to do so,[41] but the message sent by the French government nonetheless was clear.

Finally, the US government needs to elevate the importance of the PNR issue in its discussions with European officials in Brussels and member state capitals. Prospects for a broad improvement in US-EU relations could be considerably complicated by a breakdown in the 2012 US-EU agreement, with potential consequences for other important issues in the trade and security relationship.

The EU has yet to develop a definitive political and legal equilibrium between security and privacy over bulk data collection and retention for security purposes. Further action may come through legislative change or future CJEU judgments. The Luxembourg-based court prides itself on its independence from the political currents of Brussels, but it also has been known to adjust controversial aspects of its jurisprudence over time. As transatlantic air travel begins to recover from the COVID-19 pandemic, the EU is doubtless aware of the significant commercial consequences that a dispute over international PNR data transfer could engender.

The EU appears to be entering a deepening dialogue with its member states about the interaction of EU data privacy law and member state security decisions. The more that EU member states resist CJEU-imposed restrictions on their own bulk data collection and retention activities, the more they may seek solutions consistent with the interests of countries like the United States and Canada that also are subject to the effects of the court's rulings. Member states may in turn have an impact on the EU's PNR negotiating dynamic with the United States. There thus remains a path to stable and robust future transatlantic PNR data sharing, even if it will not be an easy one.

The EU likewise should consider increasing the significance of the PNR issue in its discussions with US government officials. The United States and the European Union hold regular meetings of senior justice and home affairs officials, as well as annual ministerial gatherings. Discussion of PNR data at these conclaves in recent years has become formulaic. It is time to begin substantive discussion of the issues at a higher level to preserve the transatlantic transfer of PNR data and avoid an unproductive disruption of efforts toward a better overall EU-US relationship.

---

37 Case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, EU:C:2020:790, and Joined Cases C-511/18, 512/18, and 520/18, *La Quadrature du Net and Others,* EU:C:2020:791.

38 Treaty on European Union, Article 4 (2).

39 See Theodore Christakis and Kenneth Propp, "How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States," *Lawfare*, March 8, 2021, https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states.

40 Ibid.

41 See Theodore Christakis, "French Council of State Discovers the 'Philosopher's Stone' of Data Retention," *about:intel*, April 23, 2021, https://aboutintel.eu/france-council-of-state-ruling/.

Kenneth Propp is an adjunct professor of European Union Law at the Georgetown University Law Center and a senior fellow with the Cross-Border Data Forum. He advises and advocates on data trade, privacy, security, and other regulatory issues in the United States and major international markets. From 2011-2015, he served as Legal Counselor at the US Mission to the European Union, in Brussels, Belgium, where he led US Government engagement on privacy law and policy and digital regulation, and advised on trade negotiations with the EU. In previous assignments for the Office of the Legal Adviser, US Department of State, Professor Propp specialized in legal issues relating to international criminal law and international trade and investment law. He also served as legal adviser to the US Embassy in Germany. Professor Propp holds a J.D. from Harvard Law School and a bachelor's degree from Amherst College.

The **Europe Center** conducts research and uses real-time commentary and analysis to guide the actions and strategy of key transatlantic decisionmakers on the issues that will shape the future of the transatlantic relationship and convenes US and European leaders through public events and workshops to promote dialogue and to bolster the transatlantic partnership.

The Atlantic Council's **Transatlantic Digital Marketplace Initiative** seeks to foster greater US-EU understanding and collaboration on digital policy matters and makes recommendations for building cooperation and ameliorating differences in this fast-growing area of the transatlantic economy.

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

***Forward* Defense** helps the United States and its allies and partners contend with great-power competitors and maintain favorable balances of power. This new practice area in the Scowcroft Center for Strategy and Security produces *Forward*-looking analyses of the trends, technologies, and concepts that will define the future of warfare, and the alliances needed for the 21st century. Through the futures we forecast, the scenarios we wargame, and the analyses we produce, *Forward* Defense develops actionable strategies and policies for deterrence and defense, while shaping US and allied operational concepts and the role of defense industry in addressing the most significant military challenges at the heart of great-power competition.

The Atlantic Council's **Scowcroft Middle East Security Initiative** honors the legacy of Brent Scowcroft and his tireless efforts to build a new security architecture for the region. Our work in this area addresses the full range of security threats and challenges including the danger of interstate warfare, the role of terrorist groups and other nonstate actors, and the underlying security threats facing countries in the region. Through all of the Council's Middle East programming, we work with allies and partners in Europe and the wider Middle East to protect US interests, build peace and security, and unlock the human potential of the region. You can read more about our programs at www.atlanticcouncil.org/ programs/middle-east-programs/.

This report was produced as part of the Scowcroft Center's Forward Defense practice's The Future of DHS Project, which is generously supported by SAIC. It was also made possible by general support to the Atlantic Council and from the Embassy of Bahrain to the US to the Atlantic Council's Scowcroft Middle East Security Initiative.

The Europe Center thanks Amazon Web Services for its generous support of our Transatlantic Digital Marketplace Initiative.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
*Rafic A. Bizri
*Linden P. Blue
Adam Boehler
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Teresa Carlson
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
Beth Connaughty
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
Mark T. Esper
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Amir A. Handjani
Frank Haun
Michael V. Hayden
Amos Hochstein
Tim Holt
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Robert Rangel
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Gine Wang-Reese
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of June 1, 2021

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org