Atlantic Council
FUTURE EUROPE INITIATIVE

ISSUE BRIEF

US Surveillance on Trial in Europe: Will Transatlantic Digital Commerce be Collateral Damage?

SEPTEMBER 2019 KENNETH PROPP

INTRODUCTION

In mid-July, an army of lawyers representing European Union (EU) institutions, six EU member states, and the US government convened in the ornate, gold-leaf courtroom of the European Court of Justice (ECJ) in Luxembourg to argue a case with major implications for privacy, national security, and the transatlantic digital economy. In a challenge brought by Austrian privacy activist Max Schrems, the question before the court was whether the laws governing how US intelligence agencies access personal data from Facebook users in Europe are consistent with European privacy laws. If they are not, transatlantic data-transfer mechanisms relied upon by the social network, and thousands of other companies, may be invalidated.[1] The transatlantic digital economy could suffer a nasty shock.

For more than two decades, the United States and the EU have struggled to reconcile privacy rights with the protection of national security, while sustaining digital commerce. The existing transfer arrangements reflect a fragile balance among these equities.[2] But, the tenor of the court's questioning during the July hearing suggests that this balance is at serious risk. The ECJ's judgment in the Schrems case, expected early next year, could lead to a diplomatic and legal confrontation between the EU's new leadership and a Donald Trump administration not well disposed toward the EU.

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.

1 Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, C-311/18.

2 "EU-US interactions over privacy and security have never reached a stable equilibrium," a recent study by two US political scientists concludes. Henry Farrell and Abraham L. Newman, *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security* (Princeton, NJ: Princeton University Press, 2019), 172.

Global commerce today depends on the ability of consumers and all types of companies to transfer information, including personal data, quickly and seamlessly across borders. Cross-border access to personal data is especially important for newer technologies, such as cloud computing, big-data analytics, and artificial intelligence. The United States leads the world in the fast-growing digital economy, and Europe collectively is not far behind.[3] They are each other's major digital trade partners, with the EU accounting for almost half of all US digital trade.[4] More cross-border bandwidth is devoted to data moving between the two regions than between any others worldwide.[5]

ROOTS OF THE TRANSATLANTIC PRIVACY DIVIDE

To understand how the current judicial confrontation arose, one must begin with the divergent US and EU approaches to data transfers across borders. While US privacy law places relatively few restraints on personal data located in the United States being sent abroad—and, indeed, encourages its free flow—the EU, by contrast, exercises "border control" over data transfers from Europe.[6] Under its comprehensive data-privacy law, the General Data Protection Regulation (GDPR), personal data located within the European Union may only be transferred to a third country if there is a legal arrangement in place "to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined" in other jurisdictions.[7]

The regulation sets out several alternative ways to assure the continuity of privacy protection when data are transferred outside the EU. One is a formal decision by the European Commission, the EU's executive arm, that a particular foreign country's legal regime provides an "adequate" level of protection.[8] Only a small number of countries have achieved this status, including the United States and, most recently, Japan.[9] A second is the use of "appropriate safeguards," in the form of standard contractual privacy-protection clauses that have been preapproved by the European Commission and are incorporated in contracts between parties to data transactions, with enforcement via EU member-state data-protection authorities.[10] Most transatlantic commerce relies on one of these two legal bases.

Privacy also has express constitutional protection in the EU's Charter of Fundamental Rights. The charter recognizes not only a general right to respect for private life, but also an express right to the protection of one's personal data.[11] In 2009, as part of the Lisbon Treaty reforms, the charter became the legal standard against which EU law and international agreements relating to privacy must henceforth be measured.

The European Commission first conferred adequacy on the United States in 2000, after it had negotiated the Safe Harbor Framework with the US government.[12] The framework set out agreed-upon privacy principles based on EU law, and companies pledging to uphold them were able to import EU-origin personal data into to the United States without being subject to the enforcement jurisdiction of EU member states' data-protection authorities (the Safe Harbor). Instead, the US Commerce Department oversaw these companies' compliance with the Safe Harbor principles. The Safe Harbor, first conceived by the Bill Clinton administration as a way of facilitating the emerging transatlantic digital economy, was embraced by more than five thousand companies, and was heavily utilized in transatlantic commerce for the next fifteen years.

3 Frances G. Burwell, *Making America First in the Digital Economy: The Case for Engaging Europe, Atlantic Council*, May 8, 2018, 4–5.

4 Daniel S. Hamilton, "The Transatlantic Digital Economy 2017," Center for Transatlantic Relations, 2017, viii.

5 Ibid., 51.

6 Dan Jerker B. Svantesson, International Data Privacy Law, v. 1, no. 3 (2011), 180.

7 Regulation 2016/679, Article 44. This regime for controlling export of personal data from EU territory dates back to a privacy directive adopted in 1995, and was only modestly refined by the GDPR.

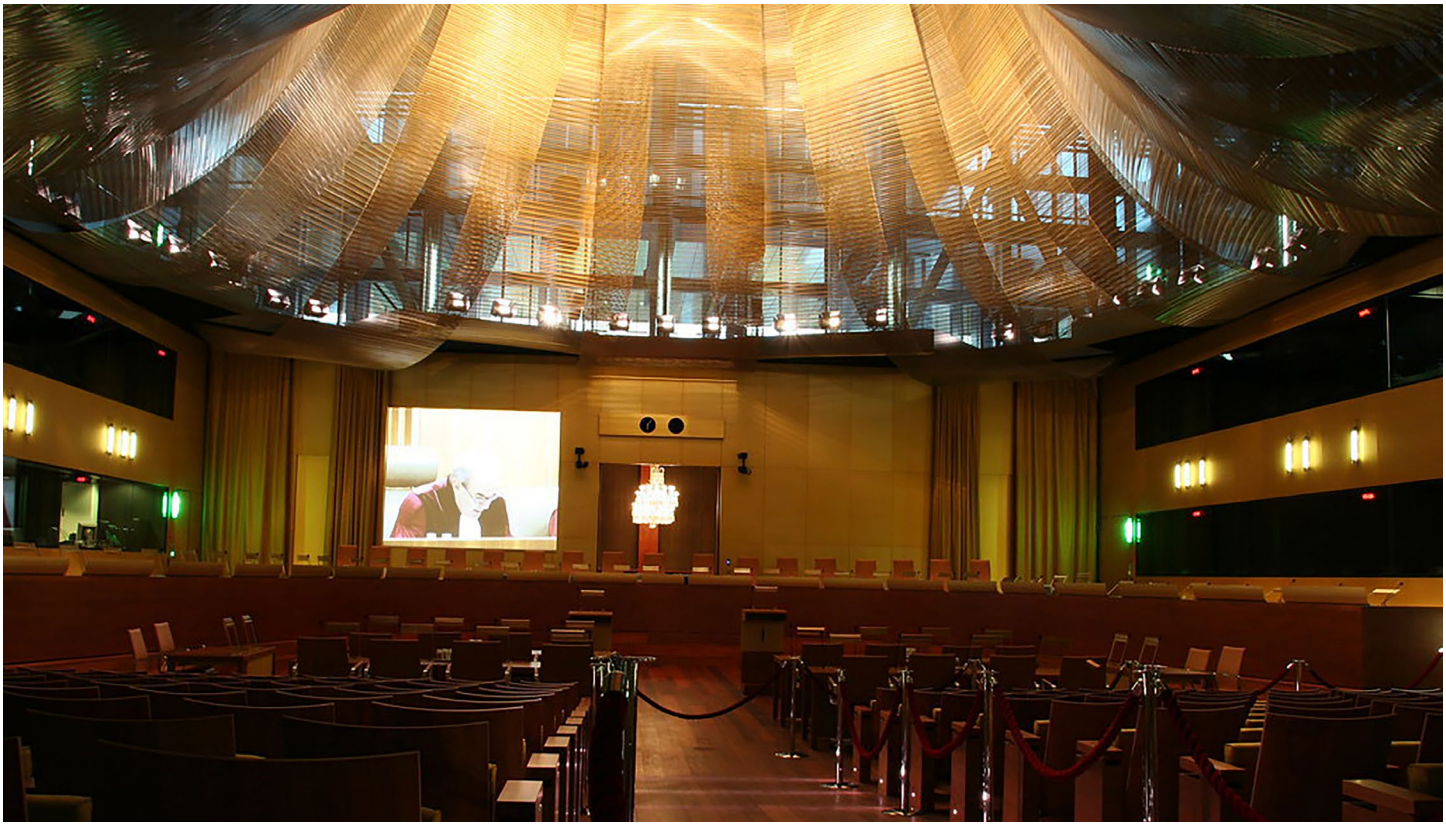
8 Ibid., Article 45.

9 The US adequacy finding only extends to transfers by companies subscribed to the US-EU Privacy Shield framework.

10 Regulation 2016/679, Article 46.

11 "Charter of Fundamental Rights of the European Union," Articles 7–8.

12 Commission Decision 2000/520/EC (July 26, 2000) pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.



Schrems' case was heard by the ECJ on July 9, 2019. The ruling, which could have major implications for the transatlantic relationship and the global economy, is expected early next year. *https://www.flickr.com/photos/puisney/3515893253*

SAFE HARBOR IS DEAD, LONG LIVE THE PRIVACY SHIELD

Edward Snowden's 2013 disclosure of the sweeping extent of US surveillance practices immediately threatened the viability of the Safe Harbor. Europeans learned that US-based communications companies and Internet service providers had turned over to the US National Security Agency (NSA) large quantities of personal data, including much that had originated in their countries. They began to wonder anxiously about the exposure of the vast trove of personal information they had shared via social networks and other digital platforms.

One European asking this question was Max Schrems, a young Austrian lawyer who had learned the techniques of legal activism while on an exchange program at a US law school. Schrems complained to the Irish data protection commissioner (DPC), the regulator of Facebook's European activities, that, in light of Snowden's revelations, the Safe Harbor did not sufficiently protect the personal data he had entrusted to the social network. The Irish courts passed the issue on to the European Court of Justice to resolve.

In 2015, the ECJ handed down a bombshell ruling. It rejected the proposition built into the Safe Harbor that a company must defer to a US surveillance request, even at the expense of violating the agreed-upon privacy principles. Further, the court asserted, a foreign country's legislation permitting its public authorities "to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life…"[13] It added that the absence of provisions in foreign legislation allowing a person

13 Maximillian Schrems v. Data Protection Commissioner, C-362/14, paragraph 94.

to have access to his or her own data, or to have it corrected or erased, denied the right to an effective judicial remedy also codified in the charter.[14] A foreign legal system could only achieve adequacy, the court ruled, if its privacy protections were "essentially equivalent" to those prevailing in the EU.[15] The court concluded that the European Commission's adequacy finding for the United States had failed to document essential equivalence—and consequently declared it invalid, with immediate effect.

The Schrems judgment sent the many companies that had been relying on the Safe Harbor scrambling overnight to find alternative legal means for their ongoing transatlantic data transfers. Most gradually shifted to standard privacy-protection clauses for their data-related contracts. During the uncertain transition, member-state data-protection authorities, encouraged by the European Commission, refrained from interrogating companies about the legal basis for their transfers.

The ruling injected new urgency and difficulty into transatlantic negotiations to revise Safe Harbor, as European Commission negotiators sought to address the ECJ's criticism of US government surveillance. Early in 2016, the governments completed a successor agreement, christened the Privacy Shield. It beefed up the privacy principles and strengthened the roles of the US Commerce Department and the Federal Trade Commission in overseeing corporate compliance, but its most important and unusual features related to US surveillance. One provision, initially suggested by the European Commission, responded to the ECJ's criticism of limited redress possibilities under US law for surveilled persons located in Europe. In a letter, the US secretary of state agreed to empower a senior deputy as an ombudsperson, to receive Europeans' surveillance-related complaints and coordinate responses with the US intelligence community.[16]

Even more extraordinary for an agreement about commercial data transfers was an accompanying pair of letters from Office of the Director of National Intelligence (ODNI) then-General Counsel Robert Litt exhaustively describing how US surveillance law operated. The letters emphasized recent changes to the US legal framework for signals intelligence, notably President Barack Obama's promulgation of a policy directive (PPD-28) that had extended some partial privacy protections to foreign nationals, and limitations on bulk collection of telephone metadata imposed by the 2015 USA FREEDOM Act. One letter also gingerly clarified that "bulk collection activities regarding Internet communications that the US Intelligence Community performs through signals intelligence operate on a small proportion of the Internet."[17]

The European Commission found the Privacy Shield a sufficient basis to grant the United States another adequacy finding, and companies in large numbers—now numbering nearly five thousand—rapidly re-subscribed to it. But, the refusal of the United States to commit in the Privacy Shield to any further changes in underlying US surveillance laws left European privacy activists unsatisfied. No sooner had the Privacy Shield taken effect in 2016 than several of them filed a new case before the General Court of the European Court of Justice, claiming that the European Commission once again had failed to restrain "generalized" US intelligence collection or to provide an effective remedy for surveilled Europeans.[18]

THE ROAD BACK TO THE ECJ

Meanwhile, Max Schrems, empowered by his unexpected success in demolishing the Safe Harbor, refocused his attention on standard contract clauses—the alternative legal transfer mechanism to which Facebook had subsequently turned. Schrems reformulated his complaint to the Irish DPC, now alleging that transfers pursuant to standard clauses were as vulnerable to US surveillance activities as those authorized by the Safe Harbor, and equally deficient from the perspective of EU fundamental rights.

The Irish DPC broadly agreed that US law was deficient, but refused to decide upon the validity of Facebook's contractual clauses, instead referring the matter back to the Irish court and urging that questions about the con-

14 Ibid., paragraph 95.
15 Ibid., paragraph 73.
16 "EU-US Privacy Shield Package," annex A.
17 Letter from General Counsel Robert Litt, Office of the Director of National Intelligence, 4.
18 La Quadrature du Net and Others v. European Commission, T-738/16.

formity of this transfer mechanism with EU law first be resolved. The Irish court undertook an in-depth inquiry of US surveillance law, hearing exhaustive presentations from expert witnesses and the US government. The Irish High Court's judgment laid out no fewer than eleven questions for the European Court of Justice to answer.[19]

Thus, the EU courts were presented with simultaneous challenges to both major data-transfer mechanisms in use with the United States, each case posing similar questions about US surveillance law and practices. In view of the commonality, the lower-instance General Court decided to temporarily defer its hearing in the Privacy Shield matter, pending resolution of the standard-clauses case by the Court of Justice.

On July 9, the Schrems II oral hearing took place before the ECJ's Grand Chamber, a fifteen-judge panel including the court's president, Koen Lenaerts of Belgium, which is reserved for the most important cases. Thomas von Danwitz, a German judge known for his expertise and activism in previous data-privacy cases, was designated as reporting judge, responsible for leading the questioning and writing the eventual judgment.

At the hearing, Max Schrems' lawyer once again took dead aim at US surveillance law. "When data is transferred by Facebook to the United States, the protection is weakened by US [surveillance] law. That is true with any transfer mechanisms, including the Privacy Shield. It's systemic," he said.[20] The US government's attorney protested that the GDPR did not give the EU license to "conduct a worldwide enquiry" of surveillance regimes across the world.[21] Several EU member states, led by Germany, chimed in to remind the court that their own surveillance activities should be considered beyond the bounds of EU jurisdiction, and that the ECJ, in any event, should not hold third countries' surveillance laws to a higher standard than their own.[22]

Facebook conceded that it complies with US government surveillance requests, but noted that they were proportionately small in relation to its data holdings. By contrast, the company's lawyer emphasized that if standard clauses were invalidated, "the effect on trade would be immense."[23] A software-industry association, the Software Alliance (also known as BSA), described to an attentive court the wide-ranging global use of standard clauses and the privacy safeguards they entail. ECJ President Lenaerts intervened to state that the court understood the importance of standard clauses and the magnitude of disruption that could result from their invalidation.

Judge von Danwitz's questions, however, were not limited to standard contract clauses—the ostensible subject of the hearing—but also ranged into the validity of the Privacy Shield. He pressed the European Commission's lawyer on whether the State Department ombudsperson was sufficiently independent of executive-branch influence to afford effective redress for Europeans' surveillance complaints. Von Danwitz also noted that the Privacy Shield did not protect personal data in transit via underseas cables from the EU to the United States, only data that had arrived.[24] Snowden had released documents describing this type of interception, which occurs without company knowledge. The EC lawyer reportedly had limited success in steering the court away from this sensitive line of questioning.

At the end of the all-day hearing, close observers came away with the sense that the ECJ might well shy away from wholesale invalidation of standard clauses, and instead simply provide guidance to the Irish DPC on how to apply them on a case-by-case basis.[25] At the

19 Reference for a preliminary ruling from the High Court (Ireland), May 9, 2018 (C-311/18).

20 Laura Kayali, "Ireland's Privacy Regulator Under Fire in EU Top Court," *Politico*, July 9, 2019, https://www.politico.eu/article/ireland-privacy-regulator-under-fire-eu-top-court-cjeu/.

21 Ibid.

22 "National security remains the sole responsibility of each Member State," according to the "Treaty on European Union," Article 4(2).

23 Kayali, "Ireland's Privacy Regulator Under Fire in EU Top Court."

24 The ODNI letters describe in detail how Section 702 of the US Foreign Intelligence Surveillance Act (FISA) provides a basis for compelling service providers to assist in NSA collection of information on non-Americans located abroad. By contrast, they only allude hypothetically to the possibility of overseas interception of communications from underseas cables, a subject governed not by US statute, but rather by Executive Order 12333.

25 However, in advance of the hearing, the European Commission, perhaps anticipating invalidation, had already begun to lay groundwork for administrative revision of standard contract clauses, starting an internal consultative process with national data-protection authorities. "Statement of European Commissioner for Justice, Consumers and Gender Equality Vera Jourova," European Commission, press release, June 13, 2019, http://europa.eu/rapid/press-release_SPEECH-19-2999_en.htm.

same time, the court seems poised to overturn the EC's adequacy decision granted to the United States in respect to the Privacy Shield, once again removing a major mechanism for transatlantic data transfers.

Even if standard clauses are granted a stay of execution from the ECJ, they might still face a lingering death. The Irish DPC and High Court have both already found that such clauses are insufficient to remedy deficiencies in US surveillance law. If the ECJ comes to a similar conclusion about the Privacy Shield, the Irish authorities would be even more inclined to suspend Facebook's transatlantic transfers via standard clauses. Similar complaints about other US companies' reliance on standard clauses would likely proliferate, in Ireland and elsewhere in Europe. The ECJ, by handing authority back to member-state DPCs on a case-by-case basis, could well be consigning standard clauses to fragmented national decisions, unending litigation, and substantial legal and business confusion.

Austrian lawyer and privacy activist Max Schrems, who successfully took on Privacy Shield's predecessor Safe Harbor in 2015, now is challenging the validity of transatlantic data transfers under contractual clauses. *https://www.flickr.com/photos/minoritenplatz8/2741445123*

CONCLUSION

All signs point to the ECJ continuing to act as a stern international protector of Europeans' privacy rights, even at the risk of once again disrupting transatlantic data transfers. While judges in Luxembourg remain focused on the perceived inadequacies of US surveillance law, there is increasingly a broader perspective in other EU quarters. Many EU member states with extensive surveillance programs of their own—including the United Kingdom, France, and Germany—appear to be growing uncomfortable with the ECJ's deepening scrutiny of the subject. Commission officials privately acknowledge that surveillance practices in authoritarian countries, notably China, may be a greater threat than the NSA to Europeans' privacy abroad.[26]

If the US government were to respond to business pressure by agreeing to negotiate a successor to the Privacy Shield, there could yet be room for compromise. There is at least a prospect that Congress could pass comprehensive US privacy legislation resembling that of the European Union in key respects, as California has recently done. Conceivably, some of the ECJ's grievances could be dealt with through the legislation—for example, by relocating the ombudsperson's role from the executive branch to an independent agency.

At the same time, US government officials are exasperated by the prospect of the ECJ again rejecting past compromises made by the European Commission in the course of negotiating data-transfer agreements. A Trump administration that has little native sympathy for the troubles of technology giants might not be disposed to renegotiate, especially if the ECJ were to demand formal reassurance regarding the interception of Europeans' data from undersea cables. On the contrary, the Trump administration could respond to demands for changes in US intelligence law by threatening or revoking the protections Europeans currently enjoy under PPD-28.

The first sign of the ECJ's likely verdict in the standard clauses case will come on December 12, when an opinion will be issued by Henrik Saugmandsgaard Øe, an advocate general (AG) at the court.[27] The subsequent ECJ judgment is expected in early 2020. The transatlantic data-privacy truce once again hangs in the balance.

Kenneth Propp *is an international lawyer who served as Legal Counselor at the US Mission to the European Union from 2011-15. He teaches European Union law at Georgetown University Law Center. He is a Non-Resident Senior Fellow with the Future Europe Initiative at the Atlantic Council.*

26 For a detailed account of China's surveillance practices and weak privacy protections, see Peter Swire, "The US, China, and Case 311/18 on Standard Contractual Clauses," *European Law Blog*, July 15, 2019, europeanlawblog.eu/2019/07/15/the-us-china-and-case-311-18-on standard-contractual-clauses/.

27 An AG opinion typically guides an ECJ judgment, but the court is not bound to follow it.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

CHAIRMAN EMERITUS
Brent Scowcroft

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
*Virginia A. Mulberger
*W. DeVier Pierson
*John J. Studzinski

TREASURER
*George Lund

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
Todd Achilles
*Peter Ackerman
Timothy D. Adams
Bertrand-Marc Allen
*Michael Andersson
David D. Aufhauser
Colleen Bell
Matthew C. Bernstein
*Rafic A. Bizri
Dennis C. Blair
Thomas L. Blair
Philip M. Breedlove
Reuben E. Brigety II
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ralph D. Crosby, Jr.
Nelson W. Cunningham
Ivo H. Daalder
*Ankit N. Desai
*Paula J. Dobriansky
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Ronald M. Freeman
Courtney Geduldig
Robert S. Gelbard
Gianni Di Giovanni
Thomas H. Glocer
Murathan Günal
John B. Goodman
*Sherri W. Goodman
*Amir A. Handjani
Katie Harbath
John D. Harris, II
Frank Haun
Michael V. Hayden
Brian C. McK. Henderson
Annette Heuser
Amos Hochstein
*Karl V. Hopkins
Robert D. Hormats
Andrew Hove
*Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Reuben Jeffery, III
Joia M. Johnson
Stephen R. Kappes
*Maria Pica Karp
Andre Kelleners
Sean Kevelighan
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Richard L. Lawson
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Wendy W. Makins
Mian M. Mansha
Chris Marlin
Gerardo Mato
Timothy McBride
John M. McHugh
H.R. McMaster
Eric D.K. Melby
Franklin C. Miller
*Judith A. Miller
Susan Molinari
Michael J. Morell
Richard Morningstar
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa-Brillembourg
Ahmet M. Oren
Sally A. Painter
*Ana I. Palacio
Kostas Pantazopoulos
Carlos Pascual
Alan Pellegrini
David H. Petraeus
Thomas R. Pickering
Daniel B. Poneman
Dina H. Powell
Robert Rangel
Thomas J. Ridge
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
Rajiv Shah
Stephen Shapiro
Wendy Sherman
Kris Singh
Christopher Smith
James G. Stavridis
Richard J.A. Steele
Paula Stern
Robert J. Stevens
Mary Streett
Nathan D. Tibbits
Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
Geir Westgaard
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
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
George P. Shultz
Horst Teltschik
John W. Warner
William H. Webster

**Executive Committee Members*

List as of June 28, 2019

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.

© 2019 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council

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

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