Atlantic Council
CYBER STATECRAFT INITIATIVE

ai x ac

April 2026

Issue brief

The US AI health data collision:
Charting the future of US cross-border data flow policy, health data, and health and biopharma AI policy

Written by Justin Sherman

This issue brief examines the intersection of US cross-border data flow policy, health data governance, and AI development in the healthcare and biopharma sectors. It explores the expanding role of health, genomic, and biometric data in AI development, the evolving US regulatory landscape governing sensitive data transfers, and the tensions between enabling innovation, protecting privacy, and safeguarding national security.

Introduction

Healthcare artificial intelligence (AI) is a promising area of AI research and development. Meanwhile, this area raises critical questions about transparency, auditability, privacy, cybersecurity, inequity, national security, and more. Data from populations across the world, from the individual to population levels, are necessary for curing disease, innovating treatment, advancing research, and assessing and responding to public health threats, among many other functions. Collecting, analyzing, and sharing health data can and does have many tangible benefits for society. Simultaneously, collecting, analyzing, and sharing health data necessarily creates risks, such as privacy risks to individuals and populations and cybersecurity risks to organizations.

The US healthcare sector is also global, underpinned by a complex international supply chain of vendors and partners, and many healthcare research efforts, trials, and other efforts depend upon access to patient data from a wide range of populations and countries. Combined, these factors make cross-border data flow policies critical to the future of US health, biopharma, and life sciences AI development, alongside the related data policy considerations.

This issue brief proceeds in three parts, looking across the roots and drivers of US cross-border data flow policy, the state of health data in the US AI sector, and future policy directions. It follows the first issue brief in this series, focused on similar issues in the European Union,[1] and comes before the next in the series, focused on similar issues in China. Key points of this brief include:

1. Mark Scott, *Navigating the European Union's AI and Health Data Framework Atlantic Council*, April 10, 2026, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/navigating-the-european-unions-ai-and-health-data-framework/.

- The drivers of American cross-border data flow policy have historically been commercial interests, consumer protection concerns, and criticisms from the European Union regarding the perceived risks to EU citizens associated with personal data transfers to the United States. More recent trends include US national security concerns about foreign adversaries' (especially China's potential) access to US personal data and US debates over AI competitiveness. The U.S. Department of Justice's (DOJ) Data Security Program and the Protecting Americans' Data from Foreign Adversaries Act (PADFAA) are notable, recent data security measures, due to their governance of cross-border data flows with a national security lens.
- The United States is home to many agencies, companies, and civil society organizations (including universities) providing a range of health datasets—sometimes directly to other entities, such as other companies or researchers; sometimes, to anyone on the internet—that entities can use to train and test AI models, from large language models (LLMs) to image recognition systems, although many cutting-edge health, genomic, and other datasets are proprietary datasets held by enterprises. While US federal law places some limits on how a few categories of entities (e.g., hospitals, health insurers) can use personal data for AI training and testing, many companies in the United States have far more freedom to use the same data for AI purposes. Future innovation areas for health data and AI technologies span disease discovery, image recognition, and protein folding, among others.
- There are at least three likely, continuous drivers of US cross-border data flow policy as it pertains to health data and health-related AI models broadly: EU-related adequacy disruptions, US government national security concerns about data transfers and touchpoints (particularly to and with China), and US government and industry narratives about an AI arms race.

Roots and Drivers of the United States' Cross-Border Data Policy

Historically, the drivers of American cross-border data flow policy have been commercial interests, consumer protection concerns, and criticisms from the European Union, in particular, the perceived risks associated with EU citizen data transfers to the United States. In recent years, while the other trends persist, US national security concerns about foreign adversaries' access to US personal data, as well as US debates over AI competitiveness, have become much more significant factors for US cross-border data flow policy. This section provides a high-level overview of the roots and drivers of US cross-border data policy, identifying major policies and themes. As discussed later, these shifts could have implications for all the data components in the AI supply chain: training data, testing data, models (themselves), model architectures, model weights, application programming interfaces (APIs), and software development kits (SDKs).[2]

A (Very) Brief History

For many years, the United States shied away from implementing substantial cross-border data flow restrictions. Many Americans and US businesses have considered this the status quo. Largely, this position has stemmed from US policy—and a related, somewhat idealistic view[3]—that the internet must remain "free" and "open," with minimal state regulations imposed on traffic or the infrastructure.[4] Cross-border data flow limits imposed from Washington would, in this view, undercut the so-called internet freedom agenda. Limits would also, in this view, impact the fast-growing US cloud computing sector—led by the so-called hyperscalers, or Amazon (AWS), Google (Google Cloud), and Microsoft (Azure)—and the many sectors, from finance to health to logistics, moving systems onto the cloud, enabling access to systems and data globally without local infrastructure.

As the European Union implemented measures over the last three-plus decades that could hinder US-EU cross-border data flows, driven at least initially by concerns about individual pri-

2. Justin Sherman, *Securing Data in the AI Supply Chain, Atlantic Council,* September 5, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/securing-data-in-the-ai-supply-chain/. See also: Kemba Walden and Devin Lynch, *The AI Tech Stack: A Primer for Tech and Cyber Policy, Paladin Global Institute,* June 2025), https://www.paladincapgroup.com/wp-content/uploads/2025/06/AI-Tech-Stack-Report.pdf.
3. Justin Sherman and Robert Morgus, *The Idealized Internet vs. Internet Realities (Version 1.0): Analytical Framework for Assessing the Freedom, Openness, Interoperability, Security, and Resiliency of the Global Internet, New America,* July 26, 2018, https://www.newamerica.org/insights/idealized-internet-vs-internet-realities/; Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (PublicAffairs, 2011).
4. See, for example: Paula Dobriansky, "Global Internet Freedom Task Force Presentation," U.S. Department of State, December 20, 2006, https://2001-2009.state.gov/g/rls/rm/78142.htm.

vacy rights,[5] the US government undertook decisive efforts to ensure those transfers could legally continue. For example, in 1995, the European Union implemented a directive on the processing of personal data and its free movement that, among others, prohibited transfers of EU personal data to countries without "adequate" levels of protection.[6] Adequacy evaluations considered the nature of the data transferred, the purpose and duration of the proposed processing operations, the country of origin and the final destination, and the final destination's rule of law and other security measures, among others. This led to a lengthy and complicated negotiation process, at the end of which the US Department of Commerce issued the Safe Harbor Privacy Principles in July 2000 and sent them to the European Commission to receive an adequacy determination.[7] Then, the Commission ruled that data transfers to the United States underneath the Safe Harbor Principles were "adequate," and thus permitted.[8] In the decade or so afterwards, cross-border data flows operated under these principles—and the United States and the European Union were able to continue reaching agreement on other aspects of cross-border data flow policy, such as promoting to other countries the importance of the free flow of information across borders and the cross-border supply of information technology and communications services.[9]

In tandem, the United States has maintained its position of a relatively open internet without cross-border data flow restrictions, while criticizing countries that went in the other direction. The 2008 National Trade Estimate called attention to regulations of international data flows and restrictions on the use of non-US data as services barriers for American companies.[10] In 2013, the National Trade Estimate specifically called out China's restrictions on cross-border data flows and rules for data sovereignty as concerning risks for non-Chinese companies.[11] The list goes on.

The biggest disruption to US-EU cross-border data flows occurred in 2013. When Edward Snowden leaked information about classified US government intelligence activities,[12] the political and popular backlash from the European Union (among other places in the world) was immense.[13] For example, one European Parliament-commissioned report stated that there was an "absence of any cognizable privacy rights for 'non-US persons' under FISA," or the United States' Foreign Intelligence Surveillance Act.[14] These leaks prompted researcher Maximilian Schrems to challenge the validity of Facebook transferring EU citizen data to the United States under the Safe

5. Note: The European Union calls this "data protection."
6. European Parliament and Council, Directive 95/46/EC 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, *Official Journal of the European Communities* L 281 (October 24, 1995), 31–50, https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng.
7. Issuance of Safe Harbor Principles and Transmission to European Commission, 65 FR 45666 (July 24, 2000), https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission.
8. European Commission, Commission Decision 2000/520/EC of 26 July 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, *Official Journal of the European Communities* L 215 (July 26, 2000), 7–47, https://eur-lex.europa.eu/eli/dec/2000/520/oj/eng.
9. See, for example: Office of the US Trade Representative, "United States-European Union Trade Principles for Information and Communication Technology Services," April 4, 2011, https://ustr.gov/callout/united-states-european-union-trade-principles-information-and-communication-technology-serv-0.
10. Office of the US Trade Representative, *2008 National Trade Estimate Report on Foreign Trade Barriers* (March 2008), 1–7, https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/archives/2008/2008-national-trade-estimate-report-fo-0.
11. Office of the US Trade Representative, *2013 National Trade Estimate Report on Foreign Trade Barriers* (March 2013), 100, https://www.ustr.gov/sites/default/files/2013%20NTE.pdf.
12. See, for example: House Permanent Select Committee on Intelligence, *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden* (H. Rept. 114-891, 114th Congress), December 2016, https://www.congress.gov/committee-report/114th-congress/house-report/891/1?outputFormat=pdf.
13. See, for example: Nick Bryant, "The Snowden Effect on US Diplomacy," BBC, October 24, 2013, https://www.bbc.com/news/world-us-canada-24664045.
14. Caspar Bowden, "The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights," PE 474.405 (European Parliament: Directorate-General for Internal Policies, 2013), https://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf.

Harbor Principles, citing the leaked information as the basis to contest the past EU "adequacy" ruling.[15] This prompted several iterations of European courts overturning US-EU cross-border data flow adequacy determinations and the United States and European Union renegotiating agreements, including the 2016 Privacy Shield Framework (after the Schrems I decision invalidated Safe Harbor) and the EU-US Data Privacy Framework, or "Privacy Shield 2.0" (after the Schrems II decision invalidated Privacy Shield).[16] Regardless of one's view of these court rulings, it is clear that they have caused significant uncertainty for EU and US data-transferring organizations—and some of this uncertainty still lingers, insofar as actual or future legal challenges to US-EU cross-border data flow adequacy develop. In September 2025, for example, the European General Court dismissed a challenge to the Framework brought by a member of the French Parliament.[17] However, it is currently on appeal to the European Court of Justice, with a possible decision ready next year.

Other notable US policy developments include processes for law enforcement access to data stored abroad and multilateral engagements to create interoperable data transfer policies. In the former case, the United States passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act in 2018, which has two core components: (1) the act allows the US government to establish executive agreements with other countries to essentially ensure, under certain rule of law criteria, that those countries' law enforcement agencies could obtain expedited, direct access to US company-held data for investigations pursuant to lawful process, while bypassing the often onerous requests under a multilateral legal assistance treaty (MLAT); and (2) it clarifies that US law can require US companies to produce data they hold or control, whether or not the infrastructure used to store the data is physically within the United States.[18] Requirements for a bilateral executive agreement included that a country's legal system must have "robust substantive and procedural protections for privacy and civil liberties" vis-à-vis law enforcement data collection, which scholars have noted resemble requirements in many countries, such as in the EU bloc's General Data Protection Regulation (GDPR) for data minimization, transparency, and accountability.[19] In the latter case, the Commerce Department, along with Canada, Japan, South Korea, the Philippines, Singapore, and Chinese Taipei, established the Global Cross-Border Privacy Rules Forum in 2022 to promote values-aligned certifications for companies to carry out compliant cross-border data transfers.[20]

Recent Moves: National Security and AI Competition Drivers

Since 2024, two major federal regulations have placed restrictions on cross-border data flows—including those within the health sector and on health data that could train and test AI systems—for national security purposes. The first is a Biden administration executive order (EO) whose implementing regulations remain operative. The second is a congressional law that expanded the Federal Trade Commission's (FTC) authorities vis-à-vis data and national security.

Drawing on authorities under the International Emergency Economic Powers Act (IEEPA), President Joseph Biden signed EO 14117, titled "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," in March 2024.[21] It said that US foreign adversaries (termed "countries of concern") can access bulk US data and use advanced technologies, including AI systems, to analyze and manipulate that data to advance national security threats, such as espionage or cyber operations. EO 14117 directed the DOJ to establish regulations that

15. See, for example, a summary at: "Data Protection Commissioner vs. Facebook (Schrems II)," Columbia University, accessed April 7, 2026, https://globalfreedomofexpression.columbia.edu/cases/data-protection-commissioner-v-facebook-schrems-ii/.
16. See, for example: Chris D. Linebaugh and Edward C. Liu, "EU Data Transfer Requirements and US Intelligence Laws: Understanding Schrems II and Its Impact on the US-EU Privacy Shield," R46724 (Congressional Research Service, March 17, 2021), https://www.congress.gov/crs-product/R46724; International Trade Administration, "Data Privacy Framework Program," U.S. Department of Commerce, accessed April 7, 2026, https://www.dataprivacyframework.gov/Program-Overview.
17. Joe Duball, ed., "European General Court Dismisses Latombe Challenge, Upholds EU-US Data Privacy Framework," IAPP, September 3, 2025, https://iapp.org/news/a/european-general-court-dismisses-latombe-challenge-upholds-eu-us-data-privacy-framework.
18. US Department of Justice. "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act,"(April 2019), 3, https://www.justice.gov/archives/opa/press-release/file/1153446/dl?inline=.
19. Peter Swire and Jennifer Daskal, "Frequently Asked Questions about the US Cloud Act," Cross Border Data Forum (CBDF), accessed April 7, 2026, https://www.crossborderdataforum.org/cloudactfaqs/.
20. US Department of Commerce, "Statement by Commerce Secretary Raimondo on Establishment of the Global Cross-Border Privacy Rules (CBPR) Forum," news release, April 21, 2022, https://www.commerce.gov/news/press-releases/2022/04/statement-commerce-secretary-raimondo-establishment-global-cross-border.
21. Exec. Order No. 14117, 89 Fed. Reg. 15421 (February 28, 2024), https://www.federalregister.gov/d/2024-04573.

specify limits on commercial transactions involving Americans' bulk sensitive personal data to protect US national security interests. The result is the DOJ's Data Security Program—what companies and others variably also call the "bulk data program" or the "data broker and national security program"—finalized in January 2025 and fully implemented in April 2025.[22]

Part of the final rule focuses on data brokerage, or the sale, licensing of access to data, or similar commercial transactions where one entity transfers data to another that did not already have it. It restricts the brokerage of two categories of data from US companies to countries of concern: bulk sensitive personal data, which can relate to any US individual with restrictions based on data-type-specific thresholds, and the US government-related data explicitly tied to individuals, such as current or former military or intelligence personnel, which is restricted regardless of the amount of data involved (i.e., no threshold). It defines the countries of concern as China, Russia, Iran, North Korea, Cuba, and Venezuela.[23]

For health-related data, the rule prohibits data brokerage if the data transferred by any entity over the preceding 12 months, in one transaction or multiple, exceeded data type-specific thresholds (pulling the below directly from the rule's text):

22. 90 Fed. Reg. 1636 (January 8, 2025), https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern.

23. For an easier summary of the rule, see: National Security Division, "Data Security Program: Frequently Asked Questions," U.S. Department of Justice, April 11, 2025, https://www.justice.gov/opa/media/1396351/dl.

Table: Categories and Thresholds for US Sensitive Personal Data

Category of "US Sensitive Personal Data"	Definitions[24]	Threshold of data collected about or maintained on:
Human genomic data	Data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a human cell, including the result or results of an individual's "genetic test" (as defined in 42 U.S.C. 300gg-91(d)(17)) and any related human genetic sequencing data.	100 US persons
Human epigenomic data	Data derived from a systems-level analysis of human epigenetic modifications, which are changes in gene expression that do not involve alterations to the DNA sequence itself. These epigenetic modifications include modifications such as DNA methylation, histone modifications, and non-coding RNA regulation. Routine clinical measurements of epigenetic modifications for individualized patient care purposes would not be considered epigenomic data under this rule because such measurements would not entail a systems-level analysis of the epigenetic modifications in a sample.	1,000 US persons
Human proteomic data	Data derived from a systems-level analysis of proteins expressed by a human genome, cell, tissue, or organism. Routine clinical measurements of proteins for individualized patient care purposes would not be considered proteomic data under this rule because such measurements would not entail a systems-level analysis of the proteins found in such a sample.	1,000 US persons
Human transcriptomic data	Data derived from a systems-level analysis of RNA transcripts produced by the human genome under specific conditions or in a specific cell type. Routine clinical measurements of RNA transcripts for individualized patient care purposes would not be considered transcriptomic data under this rule because such measurements would not entail a systems-level analysis of the RNA transcripts in a sample.	1,000 US persons
Biometric identifiers	Measurable physical characteristics or behaviors used to recognize or verify the identity of an individual, including facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints, gait, and keyboard usage patterns that are enrolled in a biometric system and the templates created by the system.	1,000 US persons
Personal health data	Health information that indicates, reveals, or describes the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. This term includes basic physical measurements and health attributes (such as bodily functions, height and weight, vital signs, symptoms, and allergies); social, psychological, behavioral, and medical diagnostic, intervention, and treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications.	10,000 US persons

24. 28 C.F.R. §§ 202.204, 202.224, and 202.241 (2025), https://www.ecfr.gov/current/title-28/chapter-I/part-202.

Importantly, the rule also introduces requirements for vendor, employment, and investment agreements vis-à-vis genomic data and personal health data (among others). It prohibits transactions that provide a country of concern or covered person with access to bulk 'omic data (i.e., genomic, epigenomic, proteomic, or transcriptomic data as defined above),[25] or to human biospecimens from which an entity could derive bulk human genomic data. Moreover, it prohibits transactions of bulk US personal health data that happen through vendor, employment, and investment agreements unless the US individual or entity carrying out the transaction complies with specified security requirements. The Cybersecurity and Infrastructure Security Agency (CISA) developed these requirements, and they span organization-, system-, and data-level protections (including data minimization and masking, encryption, or privacy-enhancing techniques). Their design is to ensure that the covered person and country of concern cannot access regulated data through this type of covered data transaction.

The DOJ's Data Security Program took effect in April 2025, but the department decided to delay enforcement 90 days until July 8, 2025, and to delay certain affirmative due diligence obligations until October 6, 2025.[26] While the team responsible for enforcing the program has lost most of its staff, the statute of limitations for any civil or criminal violation is 10 years.

The second recent national security measure for cross-border data flows is the Protecting Americans' Data from Foreign Adversaries Act (PADFAA),[27] which Congress passed in April 2024 along with the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA),[28] or the TikTok divest-or-ban law. PADFAA made it unlawful for a "data broker" anywhere in the United States to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available a US individual's "personally identifiable," "sensitive data" of a US individual to any "foreign adversary country" or any entity controlled by one.

The law's definitions of key terms determine its scope. Unlike the DOJ program, PADFAA scoped "data broker" to mean any entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available US individuals' data that the broker did not collect directly from those individuals. In other words, PADFAA defines a data broker as a third party.[29] The statute's definition of foreign adversaries comes from a list of countries in an existing (but separate) federal statute, meaning PADFAA's restrictions only apply to covered transactions to North Korea, China, Russia, and Iran (a narrower list than the DOJ program's six countries of concern).[30] Importantly, PADFAA also defined personally identifiable, sensitive data as any data that identifies or is linked or reasonably linkable, alone or in combination with other data, to an individual or a device that identifies or is linked or reasonably linkable to an individual, in multiple categories, such as government-issued identifiers, health conditions and treatments, device log-ins, sexual behavior, data on any individual under the age of 17, identifying online activity, and precise geolocation data. The law's limitations on health data sales apply to "any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual."

Hence, in some ways, the DOJ program is broader, encompassing first-party data brokers (i.e., those that collect data directly from individuals), as well as a category of low-risk transfers, while covering two additional countries (Cuba and Venezuela). In other ways, however, PADFAA is broader, equally governing all data flows within its remit (without any data-type thresholds) and covering broader categories of personal data, such as an individual's private communications (e.g., voicemails, emails, texts, direct messages). It is possible that PADFAA could affect a large corporation in the health, biopharma, life sciences, or related sectors, if that corporation were to engage in covered sales of health data it did not directly collect from consumers. Yet the DOJ Data Security Program affects these sectors much more, because it encompasses first-party collectors transferring data to the covered countries. For example, this means that many pharmaceutical companies that transfer above-threshold volumes of US citizen health data to organizations in China for health research face obligations under the regulations, subject to relevant exemptions, such as for "drug, bio-

25. Note: This excludes pathogen-specific data embedded in human 'omic datasets.
26. US Department of Justice, "Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries," news release, April 11, 2025, https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive.
27. 15 U.S.C. ch. 123 (Supp. II 2024), https://www.law.cornell.edu/uscode/text/15/chapter-123.
28. Emergency Supplemental Appropriations Act, 2024, Pub. L. 118-50, 138 Stat. 934, https://www.congress.gov/118/plaws/publ50/PLAW-118publ50.pdf.
29. Note: The DOJ's Data Security Program's definition includes both first- and third-party data sellers.
30. 10 U.S.C. § 4872(2) (2022), https://www.law.cornell.edu/uscode/text/10/4872.

logical product, and medical device authorizations" and "other clinical investigations and post-marketing surveillance data."[31] This is an important point. Companies may or may not internally make distinctions, such as in the product development or scientific research lifecycle, between some of these ways of transacting in data (e.g., is it sent via an employer agreement or another kind of transfer?) and the related purpose (e.g., it is for other clinical investigations?), but the DOJ program certainly does.

Nonetheless, these programs do not apply to any one specific part of the AI supply chain per se. If a data component in the AI supply chain—be it training data, testing data, or something else[32]—fits under the definitions of the DOJ program or PADFAA, the restrictions will enter into effect. This means they impact large training or testing datasets for various AI models and the extent to which model developers or maintainers, for example, can or cannot transfer the AI models to countries and entities of concern (and if so, under what protections).

AI innovation has heavily driven the recent discourse concerning data flows in Washington, DC—in some cases, the conceptualization of AI research and development as an "arms race" with the Chinese government (or, sometimes, framed as a technological and economic race with China writ large).[33] The debates have not yet resulted in significant legal or policy changes for cross-border data flows. For now, discourse about an "AI arms race" and innovation-regulation dynamics has mostly focused on executive branch actions targeted at the notion of preventing US states from charting their own paths in governing various AI technologies[34] (even though a wide range of states are pushing forward with AI regulations anyway).[35]

However, it is inevitable that the AI innovation discourse will affect cross-border data flows in the future. In Chatham House Rule discussions in which the author has participated, for instance, some analysts or companies have suggested that enabling certain health innovations in AI (not LLMs but beyond them) will require maintaining some degree of cross-border flows of US health data. Conversely, other Chatham House Rule discussions in which the author has participated have underscored the national security interest in further restrictions on US health, genetic, and biometric data to protect what are genuine US security interests. The bipartisan, bicameral National Security Commission on Emerging Biotechnology, to give one example, recommended in its 2025 report that Congress should conduct oversight of existing policies and add new authorities as warranted, to ensure that China cannot obtain bulk and sensitive biological data from the United States.[36] Proposals to further restrict cross-border health, genetic, and other data flows not in spite of but due to AI competition with China are likely to be salient in the coming years.

State of Health Data in the US AI Sector

The discussion around the role of health data and technology within the US AI landscape is at a critical inflection point. When the American Hospital Association surveyed thousands of hospitals around the country in 2023, 43.9 percent of hospitals in metro counties reported using some type of AI in their operations, such as for automating tasks, optimizing administrative and clinical work, and predicting patient demand.[37] In

31. 90 Fed. Reg. 1636 § 202.510 and 202.511 (January 8, 2025).
32. Note: It is less likely in this case. Other data components in the AI supply chain: models (themselves), model architectures, model weights, APIs, and SDKs. But APIs and SDKs are certainly two categories of technological mechanisms to effectuate federally regulated cross-border data transfers.
33. Note: The lines in China between the public sector and the private sector are fundamentally blurrier (or in some cases, meaningfully nonexistent) than they are in the United States—this is not to suggest otherwise. It is merely to point out the differing ways in which members of Congress, congressional staff, executive branch policymakers, think tank analysts, and so on have discussed the "AI arms race" concept of late.
34. Exec. Order No. 14365, 90 Fed. Reg. 58499 (December 11, 2025), https://www.federalregister.gov/documents/2025/12/16/2025-23092/ensuring-a-national-policy-framework-for-artificial-intelligence.
35. Cecilia Kang, "States Plow Ahead with A.I. Regulation, Defying Trump," *New York Times*, March 30, 2026, https://www.nytimes.com/2026/03/30/technology/trump-states-ai-gavin-newsom-california.html.
36. National Security Commission on Emerging Biotechnology (NSCEB), "4.2 Block China from Obtaining Sensitive U.S. Biological Data," in *Charting the Future of Biotechnology* (Final Report), United States Senate, April 2025, https://www.biotech.senate.gov/final-report/chapters/chapter-4/section-2/.
37. Nicole Summers-Gabr, "The Use of AI in the Health Care Workplace: The U.S. Experience," Federal Reserve Bank of St. Louis, July 15, 2025, https://www.stlouisfed.org/on-the-economy/2025/jul/use-ai-health-care-workplace-us-experience.

2025, by one estimate, US investors put 46 percent of their healthcare sector investments into healthcare AI companies.[38] In 2026, 75 percent of US health systems queried for a survey reported using at least one AI application, up from 59 percent the year prior.[39] Surveys can be variable, but it is clear that many US health organizations are increasingly leveraging AI models in their operations.

Data itself is another critical part of the picture. The United States has many organizations providing a range of health datasets that entities could use to help train and test AI models, from LLMs to image recognition systems. This covers two critical data components of the AI supply chain: training data and testing data.

Federal agencies publish datasets for COVID-19 tracking, de-identified patient data for cancer surveillance, medical imagery (e.g., CTs, or computed tomography scans, and MRIs, or magnetic resonance imaging) related to clinical subjects, environmental health data, multimodal genomic and electronic health records data, and much more.[40] MIT, Harvard Medical School, and Beth Israel Deaconess Medical Center researchers maintain a database of hundreds of thousands of emergency department and intensive care unit (ICU) patients' deidentified records.[41] Stanford publishes datasets of radiology reports and chest X-rays, abdominal CT scans, whole brain MRI studies, and many other kinds of health-related image training datasets.[42] Nonprofits and companies publish health data usable for AI training and testing, too: Google maintains an online "data commons" that includes health information from a wide range of sources;[43] the Radiological Society of North America runs "AI challenges" that invite researchers to develop high-performing machine learning (ML) models for specific health tasks;[44] MITRE even developed an open-source, synthetic patient generator that models the medical history of synthetic, realistic patients to create data.[45]

To whom they provide this data varies. Sometimes, these organizations provide such data directly to other entities, such as other companies or researchers. Sometimes, these organizations publicly post such data for anyone on the internet to download (with varying permissible uses). As with many datasets, an individual's or organization's access to funding (including if they need to purchase licenses for data), computing capabilities, data storage, subject matter expertise, and other informational and infrastructural resources will impact which groups can effectively leverage these datasets for health and other purposes. The widespread availability of free-to-use or low-cost AI models, including LLMs, arguably lowers many of these barriers to entry.

At the same time, many large corporations in the healthcare, biopharma, and life sciences industries have their own vast proprietary datasets, such as clinical trial data or internally developed survey data, that they can use to train AI systems that are not available to the public. One former chief data officer at three of the largest US healthcare companies recently commented, in this vein, that smaller language models trained

38. Silicon Valley Bank, "AI Investment Accounted for Nearly Half of Healthcare Investment in 2025; Silicon Valley Bank Releases 17th Healthcare Investments and Exits Report," PR Newswire, January 8, 2026, https://www.prnewswire.com/news-releases/ai-investment-accounted-for-nearly-half-of-healthcare-investment-in-2025-silicon-valley-bank-releases-17th-healthcare-investments-and-exits-report-302656179.html.
39. Cailey Gleeson, "Health System AI Adoption Surges in 2026 with Execs Reporting Increased ROI: Survey," Fierce Healthcare, March 24, 2026, https://www.fiercehealthcare.com/ai-and-machine-learning/75-us-healthcare-systems-use-plan-use-ai-platform-2026.
40. See, for example: "SEER Incidence Data, 1975–2023," National Cancer Institute, accessed April 7, 2026, https://seer.cancer.gov/data/; "Cancer Imaging Archive," National Cancer Institute, accessed April 7, 2026, https://www.cancerimagingarchive.net; "CDC Wonder," Centers for Disease Control and Prevention, accessed April 7, 2026, https://wonder.cdc.gov; "The Home of HHS Open Data," U.S. Department of Health and Human Services, , accessed April 7, 2026, https://healthdata.gov.
41. "MIMIC-IV," PhysioNet, October 11, 2024, https://physionet.org/content/mimiciv/3.1/. Note: The author, while not having personally evaluated the privacy standards of this particular dataset, observes that the most common use of "deidentified" in this context is to reference a regulatory standard that removes specific types of identifiers from the data, yet this does not mean the data is impossible to link back to specific individuals.
42. Center for Artificial Intelligence in Medicine and Imaging, "Shared Datasets," Stanford University, accessed April 7, 2026, https://aimi.stanford.edu/shared-datasets.
43. "Health," Data Commons, accessed April 7, 2026, https://www.datacommons.org/explore/health.
44. "AI Challenges," Radiological Society of North America, accessed April 7, 2026, https://www.rsna.org/artificial-intelligence/ai-image-challenge.
45. "Synthetic Patient Generation," Synthea, accessed April 7, 2026, https://synthetichealth.github.io/synthea/.

on proprietary datasets held by enterprises will deliver much more value in the future.[46] This may be especially true in some highly sensitive data categories, such as genomic data. The bigger demands for privacy and cybersecurity protections (including strict access controls—in other words, limiting the pool of people who can access the data) mean companies, universities, and even government agencies looking to develop medical and health AI models on the data may be reliant on internal datasets more than anything they can procure from a public source.[47] Health data for AI purposes in the United States, therefore, goes far beyond the text that an LLM chatbot vendor may scrape from across the internet.

For American companies seeking to use health data to train AI systems, perhaps the most significant distinction lies in whether a company is subject to the Health Insurance Portability and Accountability Act (HIPAA). Passed in 1996, HIPAA's regulations apply to four categories of entities: healthcare providers, health plans, healthcare clearinghouses, and their business associates, which include entities that provide financial, legal, accounting, or other services to a HIPAA-covered entity or that receive data from HIPAA-covered entities in conjunction with HIPAA-covered activities, such as data analysis firms or website design contractors.[48] All entities regulated by HIPAA must comply with HIPAA's privacy and security rules when seeking to train an AI system on health data, such as by ensuring it has a specialized agreement ("Business Associate Agreement") with an AI vendor before sharing any patient data.[49]

However, HIPAA does not apply to many other entities, such as social media companies, smart device manufacturers, advertising technology companies, data brokers, and many other data-collecting, -generating, and -analyzing companies. This means that many companies do not face significant federal regulations in leveraging consumers' health data for training AI applications. For example, a non-HIPAA-covered mental health app that wanted to use its own customers' data that it collected to train a predictive health model would not face HIPAA restrictions in doing so.[50] Compounding this fact is just how much health data companies collect on individuals outside the bounds of a hospital or clinic, including online purchases, smart device biometrics, and data indicating physical activity and movement levels. Such legal and regulatory gaps create significant privacy and cybersecurity risks for individuals' health data. They have also catalyzed states' interests in regulating health data with their own laws, such as Washington's My Health My Data Act,[51] to fill gaps left by decades-old federal sectoral laws. Nonetheless, many states do not have heavily health-data-focused privacy laws addressing the ways in which myriad types of data generated outside the scope of hospitals or clinics can be used for AI training purposes.

For example, OpenAI said in January 2026 that 40 million people globally use ChatGPT daily for "health information."[52] Per week, it says that about 230 million people ask the chatbot health and wellness questions.[53] Such usage is likely to continue driving legislative and regulatory concerns about the uses of US health data by AI applications, outside the scope of HIPAA and other privacy and security requirements and best practices.

Beyond commercial chatbot usage for health questions, companies, universities, and government agencies are likely to deepen their work on more specialized AI health models (including those that are smaller or trained on proprietary data) in the coming years. Google's DeepMind, through its Isomorphic

46. Bill Siwicki, "LLMs Have Their Uses, but Healthcare Needs 'Small Language Models' Too, Expert Says," *Healthcare IT News*, November 6, 2025, https://www.healthcareitnews.com/news/llms-have-their-uses-healthcare-needs-small-language-models-too-expert-says.
47. Note: While some data brokers have shown an interest in genetic data, this sector of the data brokerage market is nascent.
48. 45 C.F.R. pts. 160, 162, and 164 (as amended through March 26, 2013), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.
49. For a discussion of these regulations in the AI context, see: Delaram Rezaeikhonakdar, "AI Chatbots and Challenges of HIPAA Compliance for AI Developers and Vendors," Journal of Law, Medicine, and Ethics 51, no. 4 (Winter 2023): 988–95, https://pmc.ncbi.nlm.nih.gov/articles/PMC10937180/.
50. Note: The app must still comply with other consumer protection laws, such as the FTC's Health Breach Notification Rule. See: 16 C.F.R. pt. 318 (2024), https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule.
51. See, for example: Washington My Health My Data Act, Wash. Rev. Code § 19.373 (2023), https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true.
52. Megan Morrone, "Exclusive: 40 million People Turn to ChatGPT for Health Care," *Axios*, January 5, 2026, https://www.axios.com/2026/01/05/chatgpt-openai-health-insurance-aca.
53. Amanda Silberling, "OpenAI Unveils ChatGPT Health, Says 230 Million Users Ask about Health Each Week," *TechCrunch*, January 7, 2026, https://techcrunch.com/2026/01/07/openai-unveils-chatgpt-health-says-230-million-users-ask-about-health-each-week/.

Labs startup, has been expanding its AlphaFold protein folding model to predict the structure of proteins, DNA, and so forth.[54] Scientists at Lawrence Livermore National Laboratory, AMD, and Columbia University have developed a biological computing model, ElMerFold, run on the National Nuclear Security Administration-funded supercomputer El Capitan, to advance biosecurity efforts.[55] One company, Insitro, uses ML capabilities to analyze in vitro cellular data to identify therapeutic insights and interventions across diseases.[56] Another, Numerion Labs, uses an AI platform to analyze chemical structures to predict drug functions and other tasks.[57] These kinds of innovations are likely to become more important components of the health AI space in the coming years.

Future Policy Directions

There are at least three likely, continued drivers of US cross-border data flow policy as it pertains to health data and health-related AI models broadly: EU-related adequacy disruptions, US government national security concerns about data transfers and touchpoints (particularly to and with China), and US government and industry narratives about an AI arms race.

Currently, the EU-US Data Privacy Framework is still in place. However, other European courts could rule differently in future cases and hearings (i.e., those akin to the dismissed 2025 challenge). Many European policymakers' reactions to the last year or so of technology developments, political and policy changes, and rule of law challenges in the United States—including the calls to reduce dependence on American technology from European politicians,[58] as well as military and security agencies[59]—have generated significant debate about the nature of US-EU technological ties, including data flows and touchpoints. Nonetheless, it is not clear whether these conversations will directly translate into challenges to the Data Privacy Framework per se. The fates of any potential challenges, would be, in a word, complicated. On the one hand, for challenges filed in the current environment, the odds of invalidation based entirely on the state of US law and politics are likely much greater than in 2024. This would have ramifications for a wide range of US sectors, including the cross-border flow of health data and for health and pharma organizations working on AI applications, such as those related to drug discovery, image recognition, or patient record analysis. On the other hand, it is highly probable that the current Trump administration might pursue other means of securing adequacy besides negotiation. Other compliance questions for businesses under current frameworks, meanwhile, persist.[60]

Alongside European concerns about data transfers to the United States, here at home, the US government will likely stay focused over the next decade on the national security risks associated with the transfer of certain data to—or certain data touchpoints with—entities in China and other foreign adversary countries. Building on PADFAA and the DOJ's Data Security Program, legislators on both sides of the aisle in Congress remain interested in additional measures to bolster and expand the programs to further govern how US data can flow to China.[61] Genetic, health, and biotech-related data are of particular, heavy concern for many policymakers, because of their identifiability (especially with genetic data) and the military and intel-

54. "AlphaFold Server," Google DeepMind, accessed April 7, 2026, https://alphafoldserver.com/welcome; "The Isomorphic Labs Drug Design Engine Unlocks a New Frontier beyond AlphaFold," Isomorphic Labs, February 10, 2026, https://www.isomorphiclabs.com/articles/the-isomorphic-labs-drug-design-engine-unlocks-a-new-frontier.
55. Jeremy Thomas, "LLNL and Partners Launch Record-Breaking Protein-Folding Workflow on World's Fastest Supercomputer," Lawrence Livermore National Laboratory, November 14, 2025, https://www.llnl.gov/article/53581/llnl-partners-launch-record-breaking-protein-folding-workflow-worlds-fastest-supercomputer.
56. "Making Medicines Differently," Insitro, accessed April 7, 2026, https://www.insitro.com.
57. "Numerion Labs: Platform," Numerion Labs, accessed April 7, 2026, https://numerionlabs.ai/drug-hunting-platform/.
58. See, for example: Mathieu Pollet, "Europeans Think Trump Can Shut Do Their Internet," *Politico Europe*, March 19, 2026, https://www.politico.eu/article/europeans-donald-trump-internet-technology-us/.
59. Justin Sherman, "Europe's Talk of Dropping U.S. Tech Is Growing. How It Would Happen," *Barron's*, January 28, 2026, https://www.barrons.com/articles/europes-digital-soverignty-over-greenland-trump-threats-55fc91a9.
60. See, for example: "New Standard Contractual Clauses – Questions and Answers Overview," European Commission, accessed April 22, 2026, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en.
61. Note: Author conversations with congressional offices.

ligence contexts in which an adversary could leverage them.[62] While the current administration has articulated and pursued a clear preference for regulatory rollbacks across industries, there remains strong, underlying, bipartisan Congressional interest in national security regulations that affect health and biological data vis-à-vis China. There are also many consumer protection reasons for Congress to pass comprehensive privacy legislation that would encompass these data categories, distinct from national security per se. But the last few years have underscored that Congress is far more likely to pass piecemeal, data-focused national security laws than to make meaningful movement on a comprehensive, federal privacy framework. Members keep introducing bills, but the inching forward still runs into major roadblocks, such as debates over a private right of action.

Notably, US corporate and government discourse about the idea of an "AI race" with China will affect US health data, cross-border data flows, and data in the health AI context going forward. Many forces exist simultaneously. Some companies have a sincere belief in the need for US firms to move faster than their counterparts in China to maintain long-term American technological advantage and strategic competitiveness. Plenty of other companies, particularly in Big Tech, have also wielded these arguments instrumentally to pursue their respective ends (e.g., killing privacy regulations).[63] There are policymakers, similarly, who genuinely focus their time on the ways in which the Chinese government leverages AI for national security purposes ranging from surveillance,[64] to drone swarms,[65] and, evidently, to cyber operations.[66] There are also policymakers whose arguments about an AI arms race hinge more on the bottom lines of American firms writ large, compared to Chinese competitors, than a precisely articulated vision for what defines the supposed race.[67] All told—and without getting too much into the notion of an "AI race" itself—it is clear that future administrations will contend with these competing views of AI, competition, and China in ways that could significantly relax or tighten the US regulatory apparatus for health data, AI models such as image recognition or genomic data analysis, and cross-border data flows.

Looking forward, the challenge for policymakers, as is often the case in policymaking, lies in doubling down on areas where important interests align, while navigating balancing acts where they diverge. The challenge for health, biopharma, and related AI companies will include deepening their understanding of, appreciation for, and fluency in issues related to US national security, AI competition, and China. And the challenge across the board, including for non-US entities and those in civil society, will be the thoughtful critique of the overarching framings that guide US policy in this area to ensure calibrated, evidence-based measures based on clear, genuine intentions from the promoters of those rhetorical framings. This could include considering:

- "AI" is an umbrella term that encompasses a wide range of technologies, far beyond the LLM chatbot makers that dominate the headlines, stock market reports, and policy conversations. Relatedly, there are many different use cases for AI models, including non-LLM AI mo-

62. See, for example: Prohibiting Foreign Access to American Genetic Information Act of 2024, S.3558, 118th Congress (2024), https://www.congress.gov/bill/118th-congress/senate-bill/3558/text; United States House of Representatives Select Committee on China, "Moolenaar, Krishnamoorthi, Dunn Recommend Strengthened Controls to Prohibit the PLA from Accessing U.S. Clinical Trial Data," news release, January 10, 2025, https://chinaselectcommittee.house.gov/media/press-releases/moolenaar-krishnamoorthi-dunn-recommend-strengthened-controles-to-prohibit-the-pla-from-accessing-us-clinical-trial-data; Krysta Escobar, "'Terrifying': Why U.S. Senator in Top Intel Post Wants More Spying on Chinese Companies," CNBC, December 6, 2025, https://www.cnbc.com/2025/12/06/china-us-technology-spying-senate-concerns.html.

63. Justin Sherman, "Don't Be Fooled by Big Tech's Anti-China Sideshow," *WIRED*, July 30, 2020, https://www.wired.com/story/opinion-dont-be-fooled-by-big-techs-anti-china-sideshow/.

64. See, for example: "China's Algorithms of Repression," Human Rights Watch, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass; Dave Davies, "Facial Recognition and Beyond: Journalist Ventures Inside China's 'Surveillance State,'" NPR, January 5, 2021, https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta; Paul Mozur and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers," *New York Times*, December 17, 2019, https://www.nytimes.com/2019/12/17/technology/china-surveillance.html.

65. Timothy Ditter, "China Readies Drone Swarms for Future War," Center for Naval Analyses (CNA), September 24, 2025, https://www.cna.org/our-media/indepth/2025/09/china-readies-drone-swarms-for-future-war.

66. "Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign," Anthropic, November 13, 2025, https://www.anthropic.com/news/disrupting-AI-espionage.

67. Tristan Bove, "America Could 'Lose the AI Race' Because of Too Much 'Pessimism,' White House AI Czar David Sacks Says," Fortune, January 22, 2026, https://fortune.com/2026/01/22/david-sacks-warns-america-could-lose-the-ai-race-because-of-pessimism/.

dels, which have quite varied impacts on society. In this case, LLMs built by commercial chatbot vendors and pitched as health tools are different than LLMs built by clinical researchers and trained, methodically and precisely, for specific tasks—or image recognition systems built by healthcare companies to screen for cancer. Unpacking these distinctions in regulatory discussions will be critical to differentiating between risks, opportunities, and types of societal and individual impact. This kind of differentiation may be easier with organizations developing focused AI models that use specific types of data for specific purposes, compared to, say, LLM vendors pitching their tools as general-purpose and thus (at least purportedly) cutting across many different use cases.

- Healthcare is not the same as advertising. Policymakers may regulate or want to regulate cross-border data flows and "AI" with only a particular kind of AI technology or AI use case in mind, such the privacy risks of LLM vendors marketing chatbots as therapy solutions for teenagers (which the American Psychological Association warns against)[68] and turning those conversations into ad insights—or social media platforms using users' health data to target them with AI-driven, problematic advertisements. Yet, the resulting regulations could also implicate use cases that are less about data ingestion or commercial advertising and more about, say, disease research or clinical trial development. It is not mutually exclusive that policymakers could curtail harms in one area while understanding the public health implications and other related consequences of broader regulations in other areas.
- Many companies lack a deep understanding of the national security risks associated with business activities in or technological ties to China. This could mean the US government should provide more opportunities for companies to understand the risk space. Rather than declassifying significant volumes of intelligence or providing companies with hyper-specific lists of static risk criteria (e.g., for national security regulatory programs), this could look like the government issuing more plain-language justifications for data-related regulatory decisions.[69] It could look like federal regulators issuing more advisory opinions for the growing number of federal data-related regulatory programs. And it could look like federal agencies meeting more with companies outside of investigations.[70] At the same time, there are often fundamentally divergent perceptions of the risk environment (or the valuation placed on what the US government sees as national security risks) that it is unlikely this gap will close entirely—and some US national security-motivated data regulations will address issues that companies may to some extent be in tension with.
- Beyond the moral and societal reasons to continually explore advancements in health technology, policymakers and other stakeholders should note that health data and health-related AI developments could also have beneficial applications for biosecurity as well, aligning with US national security interests across homeland security, national defense, and more. Framing commercial innovation, societal benefit, and national security interests as always inherently in tension is often an imprecise way of approaching problems, which can obscure complex solutions.

68. Zara Abrams, "Using Generic AI Chatbots for Mental Health Support: A Dangerous Trend," American Psychological Association, March 12, 2025, https://www.apaservices.org/practice/business/technology/artificial-intelligence-chatbots-therapists.
69. For non-data transfer-related examples in the national security space, see: Bureau of Industry and Security, "Kaspersky Lab, Inc. Prohibition," U.S. Department of Commerce, accessed April 22, 2026, https://www.bis.gov/kaspersky; U.S. Department of Justice, "Team Telecom Recommends the FCC Deny Application to Directly Connect the United States to Cuba through Subsea Cable," news release, November 30, 2022, https://www.justice.gov/archives/opa/pr/team-telecom-recommends-fcc-deny-application-directly-connect-united-states-cuba-through.
70. Note: These are all issues surveyed in Justin Sherman, *Navigating Technology and National Security: The Intersection of CFIUS, Team Telecom, AI Controls, and Other Regulations* (Wiley, 2025).

About the author

Justin Sherman is a nonresident senior fellow at the Atlantic Council's Cyber Statecraft Initiative. He is also the founder and CEO of Global Cyber Strategies, a Washington, DC-based research and advisory firm, a contributing editor at *Lawfare*, and a columnist at *Barron's*. He is the author of the book *Navigating Technology and National Security*.

Acknowledgments

The author would like to thank Ken Propp, Lee Licata, Jolynn Dellinger, Stacey Gray, and Trey Herr for their comments on earlier drafts of this report, various health and biopharma sector experts for background discussions, and Nitansha Bansal, Kenton Thibaut, and the rest of the project team for their support.

About the center

The **Cyber Statecraft Initiative** works at the nexus of geopolitics, technology, and security to craft strategies to help shape the conduct of statecraft and to better inform and secure users. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

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
1400 L Street NW, 11th Floor
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org