Fall 9-2023

Two Visions of Digital Sovereignty

Sujit Raman

Two Visions of Digital Sovereignty[1]

Sujit Raman[2]

If bipartisan agreement in the United States is rare, in at least one area, it is increasingly clear: "economic security[3] is national security."[4] As global events have pushed Europe and the United States closer together, the convergence of these concepts[5]—both at home and abroad—has begun shifting the tenor of the long-turbulent transatlantic relationship.

Consider cross-border data flows. In the recent past, issues concerning digital trade and digital security—from who creates, derives value from, and accesses data, to how it is shared, where it's stored, and for how long—gave rise to considerable friction[6] and persistent misunderstanding.[7] Today, those same issues provide glimpses of opportunities for transatlantic collaboration[8] and the development of mutual trust.[9]

The good news is that policymakers on both sides of the Atlantic appear to recognize the possibilities of a moment in which digital commerce issues run parallel to, and perhaps even coterminously with, digital security issues, and in which the two can be mutually reinforcing. (If

---

[1] This piece was first published online at Lawfare on June 1, 2023. It is available at www.lawfaremedia.org/article/two-visions-of-digital-sovereignty.

[2] The author is the chief legal officer of a global technology company and a senior fellow in the Tech, Law & Security Program at the American University in Washington, D.C.

[3] *See* Off. President, National Security Strategy of the United States of America: December 2017, 3-4 (2017) (describing the protection of economic stability and growth as part of overall national security).

[4] *See* Off. President, Interim National Security Strategic Guidance: March 2021, 9 (2021) (treating economic prosperity as one of the country's "national security priorities").

[5] David H. McCormick, Charles E. Luftig & James M. Cunningham, *Economic Might, National Security, and the Future of American Statecraft*, 3 Tex. Nat'l. Sec. Rev. 51, 52 (2020).

[6] *See* Nigel Cory & Ellysse Dick, How to Build Back Better the Transatlantic Data Relationship, Info. Tech. & Innovation Found., 2 (2021), https://itif.org/publications/2021/03/25/how-build-back-better-transatlantic-data-relationship/ (explaining, "transatlantic digital policy cooperation has faced a decade of turmoil").

[7] European Parliament Memorandum PE 652.073, The CJEU judgment in the Schrems II case (Sept. 2020).

[8] *See* Nat'l Inst. of Standards and Tech., TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management 1-3 (Dec. 1, 2022) (advocating for the potential of mutually beneficial framework agreements between the United States and European Union regarding artificial intelligence).

[9] *See* Press Release, Off. President, *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, Off. President (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ (expressing commitment to the new Trans-Atlantic Data Privacy Framework with the European Union, which establishes new standards for transatlantic data sharing practices).

nothing else, the recent record 1.2 billion euro fine against Meta[10] should accelerate implementation[11] of the new EU-U.S. Data Privacy Framework (DPF).)[12]

But if momentum on transatlantic data issues is to last over the long run, at least one concept popular in recent European policy discourse will need to be reimagined. That concept—"immunity[13] to non-EU law"[14]—refers to the idea that any private-sector entity, in order to be entrusted with storing sensitive EU data, must be subject exclusively to EU jurisdiction and, therefore, must be "independent" of the concurrent reach (including for legitimate law enforcement purposes) of any foreign sovereign's law.

This immunity concept is integral to a pending EU cybersecurity[15] proposal[16] that also would require the localization of sensitive data within Europe and would impose strict citizenship and control requirements on qualifying cloud service providers (CSPs). Typically justified in security terms, such provisions would subject the relevant data to heightened, rather than diminished, cybersecurity risk. And by "practically excluding American and other international cloud providers"[17]—including, perhaps unwittingly, the leading EU-based providers, as well—"from the EU market," these requirements would have a hard-edged commercial impact. Most importantly, the contemplated immunity requirements could have a catastrophic impact on transatlantic data flows generally and on the DPF specifically. At bottom, "immunity to non-EU law" is an artifact of the not-too-distant past in which "digital sovereignty"[18] essentially meant digital autarky and in which ideas regarding digital commerce and digital security mixed in confused, often misinformed ways—usually to the detriment of both.

---

[10] Hannah Murphy & Javier Espinoza, *Facebook Owner Meta Hit with Record €1.2bn Fine over EU-US Data Transfers*, Financial Times (May 22, 2023), https://www.ft.com/content/d1607121-0a2e-4b74-b690-d368d0c290e8.
[11] Andrea Vittorio, *Meta's $1.3 Billion Privacy Fine Propels US-EU Data Plan (1)*, Bloomberg Law (May 23, 2023, 5:05 AM), https://news.bloomberglaw.com/privacy-and-data-security/metas-record-privacy-fine-propels-us-plan-for-eu-data-disputes.
[12] Rachel F. Fefer & Kristin Archick, Cong. Rsch. Serv., IF11613, U.S.-EU Trans-Atlantic Data Privacy Framework (June 2, 2022).
[13] *See* Online Trust Coalition, Non-paper by DE, ES, FR and IT on the EUCS Requirements for Immunity to Non-EU Laws, (2021) (proposing revisions to the European Union Cloud Services Scheme, or "EUCS").
[14] Le Cloud pour les administrations [The Cloud for Government], République Française [French Republic], https://www.numerique.gouv.fr/services/cloud/regles-doctrine/ (Fr.) (last visited Aug. 16, 2023).
[15] Lucca Bertuzzi, *EU Cloud Certification Headed for Tiered Approach on Sovereignty Criteria*, Euractiv (May 12, 2023), https://www.euractiv.com/section/cybersecurity/news/eu-cloud-certification-headed-for-tiered-approach-on-sovereignty-criteria/.
[16] *See generally* European Union Agency for Cybersecurity, *Draft Version of the Cloud Services Scheme*, at 17-18, (May 2023) (describing the benefits of the tentative legal scheme that would impose new legal restrictions onto cloud service providers).
[17] Vincent Voci et al., *Issue Briefing: The European Union's Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS): How "Sovereignty" Requirements Undermine Cybersecurity and Harm Transatlantic Ties*, U.S. Chamber of Commerce, (Dec. 5, 2022), https://www.uschamber.com/security/cybersecurity/issue-briefing-the-european-unions-proposed-cybersecurity-certification-scheme-for-cloud-services-eucs (criticizing the proposed Cloud Services Scheme as actually creating discriminatory business and competitive advantages favoring European entities).
[18] European Parliament Memorandum PE 651.992, Digital Sovereignty for Europe (July 2020).

There is another way. An alternative vision of digital sovereignty has long existed, a vision in which rule-of-law nations work together to lower barriers to the free flow of digital trade and of digital evidence for law enforcement and public safety purposes, even as they build robust, consensus-based frameworks of trust premised on shared values (like individual privacy and due process) and respectful of sovereign differences. That vision has experienced renewed life recently, including in Europe. Policymakers should take concrete steps to expand its domain.

Streamlined Access, Increased Privacy Protections

For those working on transatlantic data issues, these are heady days. After nearly two years of uncertainty[19] wrought by the *Schrems II* decision[20], the EU and the United States announced a new data privacy framework[21] in March 2022 that, "[b]y ensuring a durable and reliable legal basis for data flows," aspires to "underpin an inclusive and competitive digital economy and lay the foundation for further economic cooperation." As promised, an October 2022 executive order[22], along with an intelligence community implementing directive[23] and a U.S. Department of Justice rulemaking[24], introduced new privacy and civil liberties safeguards in connection with U.S. signals intelligence programs. For its part, the European Commission in December launched[25] the process[26] for finding that the new framework provides an "adequate level of data protection" under the General Data Protection Regulation (GDPR)[27], Europe's data protection

[19] Theodore Christakis, *After* Schrems II*: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe,* European Law Blog (July 21, 2020), https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/.
[20] Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd., ECLI:EU:C:2020:559 (July 16. 2020).
[21] Press Release, Off. President, *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework* (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.
[22] Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 7, 2022).
[23] Off. Dir. Nat'l Intel., Intelligence Community Directive 126: Implementation Procedures for the Signals Intelligence Redress Mechanism under Executive Order 14086, (Dec. 6, 2022).
[24] 28 C.F.R. § 201 (2022).
[25] European Commission Press Release IP/22/7631, Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US (Dec. 13, 2022). https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631.
[26] European Commission, *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection*, European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Aug. 23, 2023).
[27] Intersoft Consulting, *General Data Protection Regulation GDPR,* Intersoft Consulting, https://gdpr-info.eu/ (last visited July 26, 2023).

and privacy law regime. Despite recent[28] hiccups[29], that process[30] continues apace[31] and is expected to conclude (positively) in the coming months.

As transatlantic commercial data flows begin to find a firmer and hopefully more permanent legal footing—mirroring the "booming" trade and investment ties[32] between the U.S. and Europe; the growing recognition[33] of shared[34] security interests[35]; and the creation of joint governmental initiatives like the U.S.-EU Trade and Technology Council[36], a bilateral forum[37] designed to "advance a multilateral economic order that privileges ties and economic exchange between aligned countries that share a plurality of interests and values"—efforts to build a more efficient yet privacy-protective EU-U.S. information-sharing framework for law enforcement and national security purposes likewise seem poised to find new life.

Such efforts could build upon several recent milestones:

---

[28] European Parliament Memorandum PE 740.749v01-00, Draft Motion to Wind up the Debate on the Statement by the Commission Pursuant to Rule 132(2) of the Rules of Procedure for a Resolution on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework (2023/2501(RSP)) (Feb. 14, 2023).

[29] *See* European Parliament, European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)) (May 11, 2023) (describing "mass surveillance" as "indiscriminate collection of data" that is "detrimental to the trust of European citizens' and businesses' trust in digital services").

[30] Int'l Ass'n Priv. Pro., From Privacy Shield to the Trans-Atlantic Data Privacy Framework, https://iapp.org/media/pdf/resource_center/privacy_shield_trans_atlantic_data_privacy_framework_infographic.pdf (April 2022).

[31] *See* Eur. Data Prot. Bd., *EDPB Welcomes Improvements under the EU-U.S. Data Privacy Framework, but Concerns Remain* , European Data Protection Board (Feb. 28, 2023), https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en (showing the EDPB's recognition that the U.S. had made "significant improvements" to its data collection practices due to the President issuing Executive Order 14086 earlier in October of 2022).

[32] Tom Fairless, *U.S.-Europe Trade Booms as Old Allies Draw Closer: Russia's attack on Ukraine and China's economic travails are encouraging a trade and investment renaissance*, Wall St. J. (Nov. 22, 2022, 5:30 AM), https://www.wsj.com/articles/u-s-europe-trade-booms-as-old-allies-draw-closer-11668914679.

[33] *See* Dave Lawler, *U.S. and EU Positions on China are Converging, Top Official Says*, Axios (Dec. 5, 2022), https://www.axios.com/2022/12/05/eu-us-china-positions-converge-trade-security (reporting that the EU and the U.S. "reached a common assessment of the challenges posed by China").

[34] Walter Lohman, *Biden's Trip to Europe and the Future of Transatlantic Cooperation on China*, Heritage Found. (Jun. 29, 2021), https://www.heritage.org/asia/commentary/bidens-trip-europe-and-the-future-transatlantic-cooperation-china.

[35] Foo Yun Chee, *European Parliament latest EU Body to Ban TikTok from Staff Phones*, Reuters (Feb. 28 2023), https://www.reuters.com/technology/european-parliament-ban-tiktok-staff-phones-eu-official-says-2023-02-28/.

[36] Off. U.S. Trade Representative, *U.S.-E.U. Trade and Technology Council (TTC)*, Exec. Off. Pres. https://ustr.gov/useuttc (last visited July 26, 2023).

[37] Thomas J. Duesterberg & Angélique Talmor, *The Potential Role of the US-EU Trade and Technology Council in a Rapidly Changing Global Economic Order*, Hudson Inst. (June 16, 2022), https://www.hudson.org/foreign-policy/the-potential-role-of-the-us-eu-trade-and-technology-council-in-a-rapidly-changing-global-economic-order.

➢ Last December, the Organization for Economic Cooperation and Development[38] (OECD) adopted "the first intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes." Two years in the making, the OECD declaration[39]—which has been endorsed by 38 countries (including the United States) and the European Union—"stemmed from growing concerns that the absence of common principles in the sensitive domains of law enforcement and national security could lead to undue restrictions on data flows." By finding areas of consensus linking the long-term future of digital commerce to discussions surrounding government access-to-data issues, the project helps create trust in cross-border data flows among democratic, rule-of-law nations.

➢ The OECD declaration followed in the footsteps of the opening for signatures in May 2022 of another long-running multilateral project concerning rule-of-law nations' access to data for law enforcement purposes: the Second Additional Protocol[40] to the Budapest Convention on Cybercrime[41]. That protocol—which, to date, has been signed by over 30 nations[42] (including the United States and numerous Council of Europe countries)—is, according to the U.S. Department of Justice[43], "specifically designed to help law enforcement authorities obtain access to ... [cross-border] electronic evidence, with new tools including direct cooperation with service providers and registrars, expedited means to obtain subscriber information and traffic data associated with criminal activity, and expedited cooperation in obtaining stored data in emergencies"—all "subject to a system of human rights and rule of law safeguards." (To be sure, some[44] privacy advocates[45] have a less sanguine view.)

---

[38] Org. for Econ. Co-operation and Dev., *Landmark Agreement Adopted on Safeguarding Privacy in Law Enforcement and National Security Data Access*, Org. for Econ. Co-operation and Dev., (Dec. 14, 2022), https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm#:~:text=The%20OECD%20Declaration%20on%20Government,access%20personal%20data%20under%20existing

[39] Org. for Econ. Co-operation and Dev., Declaration on Government Access to Personal Data Held by Private Sector Entities, Org. for Econ. Co-operation and Dev. (Dec. 13 2022), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

[40] Counc. Eur., *Details of Treaty No.224*, Council of Europe (2023), https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224.

[41] Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185.

[42] Counc. Eur., *Chart of signatures and ratifications of Treaty 224*, Council of Europe (2023), https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224.

[43] Press Release, Off. Pub. Affr's, *United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime*, U.S. Dep't Just. (May 12, 2022), https://www.justice.gov/opa/pr/united-states-signs-protocol-strengthen-international-law-enforcement-cooperation-combat.

[44] *See* Katitza Rodriguez & Karen Gullo, *Cross-Border Access to User Data by Law Enforcement: 2021 Year in Review*, Elec. Front. Found. (Jan. 3, 2022), https://www.eff.org/deeplinks/2021/12/cross-border-access-user-data-law-enforcement-year-review-2021 (remarking that Second Additional Protocol makes certain groups more vulnerable, including journalists and activists and also straightforwardly warning that law enforcement agencies have "their holiday wish list").

[45] Eur. Data Prot. Bd., *Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention),* European Data Protection Board (Feb. 2, 2021), https://edpb.europa.eu/sites/default/files/files/file1/statement022021onbudapestconventionnewprovisions_en.pdf (noting, among other considerations, a potential ambiguity concerning whether a signatory is bound to adhere to Article 15 of the Convention on Cybercrime "in the context of . . . cross-border cooperation").

➢ Earlier this year, the EU Council and the European Parliament finally reached agreement[46] on an intra-EU "e-evidence" framework[47] for cross-border access to electronic evidence. This long-debated regulation will allow public authorities in one EU member state to issue judicial orders requiring the production of electronic evidence directly on service providers located in another member state, thereby bypassing traditional, often-cumbersome mutual legal assistance mechanisms, without prejudice to fundamental individual rights.

➢ Shortly thereafter, in early March 2023, the EU and the U.S. jointly announced[48] the "resumption of negotiations[49]"—which were stalled in recent years[50] while the e-evidence framework was being worked out—"on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations." Those negotiations will likely be guided, at least in part, by similar agreements that the U.S. government has recently executed with the United Kingdom[51] and with Australia[52], which streamline mutual access to data for law enforcement and national security purposes while acknowledging and accommodating each sovereign's sometimes-diverging "essential[53] interests[54]." U.S. and EU negotiators could also draw inspiration from ongoing[55] frameworks[56], negotiated in the pre-GDPR era, that "introduced high privacy safeguards[57] for transatlantic law enforcement cooperation" and "provide[] for the

[46] Press Release, Counc. Eur. Union, *Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence*, (Jan. 25, 2023 10:10 A.M.).
[47] Council of the European Union Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM (2018) 225 (Jan. 20, 2023).
[48] Press Release, Off. Pub. Affr's, *Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations*, U.S. Dep't Just., (Mar. 2, 2023).
[49] Press Release, Off. Pub. Affr's, *Joint US-EU Statement on Electronic Evidence Sharing Negotiations*, U.S. Dep't Just., (Sept. 26, 2019).
[50] *See* Kenneth Propp, *Has the Time for an EU-U.S. Agreement on E-Evidence Come and Gone?*, Lawfare (June 2, 2022 1:33 P.M.), https://www.lawfaremedia.org/article/has-time-eu-us-agreement-e-evidence-come-and-gone (describing EU and U.S. negotiations as being in a "deadlock").
[51] Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, Oct. 3, 2019, CS USA No. 6/2019.
[52] Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, Dec. 15, 2021.
[53] Minister of State for Security Statement UIN HCWS25, UK-US Data Access Agreement (Oct. 21, 2019).
[54] Parliament of the Commonwealth of Australia Report, Report 204 on Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (Dec. 2022).
[55] Council Decision (EU) No. 2016/920 of May 20 2016, 2016 O.J. (L 154).
[56] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, June 28, 2010, O.J. (L 8/11).
[57] Eu. Comm., *EU-US Data Transfers: How Personal Data Transferred between the EU and US is Protected*, Eu. Comm., https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en (last visited July 28, 2023).

appropriate safeguards[58] to accommodate legitimate concerns about security, privacy, and respect [for] fundamental rights."

➤ Most recently, in late April, the digital and technology ministers of the Group of Seven (G-7) nations met in Japan and "reaffirm[ed] [their] commitment"[59] to facilitating cross-border data flows and to addressing challenges "regarding security, privacy protection, [and] data protection[.]" Notably, the participating ministers established a formal Institutional Arrangement for Partnership[60] (IAP) designed to enhance trust in cross-border data flows. While the scope of the IAP has not yet been set, it could serve as a mechanism to better align trusted data policies between the EU and the rest of the G-7 nations, including the United States.

Overall, while broader tensions[61] in the relationship surely remain[62], recent trends around transatlantic data flows are encouraging. Both the United States and the EU are prioritizing the formalization of mechanisms to streamline how they access data stored outside their borders needed for law enforcement, national security, and regulatory purposes. This is a fundamental necessity in an age when businesses store data around the globe for beneficial reasons and when digital evidence is likewise borderless. Such mechanisms advance sovereign interests in the efficient enforcement of domestic law and in the preservation of public safety, consistent with civil rights and civil liberties protections. And all of this is being accomplished in tandem with a related project aimed at broadening cross-border commercial access to data for trade and innovation.

A More Bounded Vision

Despite these recent trendlines, a separate, very different vision of European digital sovereignty persists. That vision (to which I'll refer as the "sovereignty-based approach") derives from

---

[58] Eu. Comm., *Migration and Home Affairs: Terrorist Finance Tracking Programme*, Eu. Comm., https://home-affairs.ec.europa.eu/pages/page/terrorist-finance-tracking-programme_en#:~:text=The%20EU-US%20TFTP%20Agreement%2C%20which%20took%20effect%20on,about%20security%2C%20privacy%20and%20respect%20of%20fundamental%20rights (last visited July 28, 2023).

[59] Min. Internal Affr's and Commcn's, Ministerial Declaration of the G7 Digital and Tech Ministers' Meeting, at 1 ¶ 3, Hiroshima Summit (April 20, 2023).

[60] *Id*.

[61] Nigel Cory & Robert D. Atkinson, *How to Build Back Better the Transatlantic Data Relationship*, Info. Tech. & Innovation Found., https://itif.org/publications/2022/12/02/hope-for-the-best-but-prepare-for-the-worst-at-the-us-eu-trade-and-technology-council/ (Dec. 2, 2022).

[62] *See e.g.* Kenneth Propp, *The big problems you won't hear about at the EU-US Trade and Technology Council*, New Atlanticist Blog (Dec. 2, 2022), https://www.atlanticcouncil.org/blogs/new-atlanticist/the-big-problems-you-wont-hear-about-at-the-eu-us-trade-and-technology-council/ (noting EU skepticism over U.S. subsidies for electric vehicle manufacturers as part of the Inflation Reduction Act of 2022).

prominent calls in recent years for European "strategic autonomy[63]" and demands for such autonomy to extend[64] into the realm[65] of[66] "technological sovereignty."[67]

Officially, the sovereignty-based approach is premised largely on the need for data security, especially in connection with information "of national importance"[68] that is stored in the cloud. Maintaining information security is indisputably important for any government. It is also critically important for any private firm storing such information on a government's behalf. Maintaining data autonomy is also an understandable strategic priority; in light of[69] recent[70] events,[71] it may be unsurprising that European officials[72] are factoring in "the possibility of ... getting cut off[73] from American cloud services" as they decide how and where to store sensitive data. And yet, as explained below, a sovereignty-based approach actually imperils the security of such information rather than protects it. Such an approach also weakens collective defense against malign cyber activity precisely at a time when, more than ever, rule-of-law nations need collaboration between private- and public-sector entities.[74]

More broadly, critical aspects of the sovereignty-based approach suffer from incoherence. According to its proponents, this approach ensures data security and autonomy because it requires sensitive European data to be stored on European soil by European-owned and European-staffed CSPs that maintain their headquarters in the EU. Proponents believe that CSPs stockaded in this way will be subject only to EU law and will therefore be "immune to non-EU

---

[63] Raluca Csernatoni, *The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty*, Carnegie Eur. (Aug. 12, 2021), https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134.
[64] Charles Michel, President, Eur. Counc., Speech at Masters of Digital 2021: Digital sovereignty is central to European strategic autonomy (Feb. 3, 2021).
[65] Ursula Von Der Leyen, President, Eur. Comm'n, State of the Union Address (Sept. 16, 2020).
[66] Ursula Von Der Leyen, President, Eur. Comm'n, State of the Union Address (Sept. 15, 2021).
[67] Thierry Breton, Comm'r for Internal Mkt. Eur. Union, Eur. Comm'n, Speech to European Commission: Sovereignty, self-assurance and solidarity: Europe in today's geopolitics (Sept. 5, 2022).
[68] Chakib Kissane, *SecNumCloud: the Certification for Cloud Confidence Service Providers*, Oodrive: Security Blog (Aug. 24, 2023), https://www.oodrive.com/blog/security/secnumcloud-the-certification-for-cloud-confidence-service-providers/.
[69] Swift, *An Update to Our Message for the Swift Community*, Swift (Mar. 20, 2022), https://www.swift.com/news-events/news/message-swift-community.
[70] Matthew Prince, *Blocking Kiwifarms*, Cloudflare: Cloudflare Blog (Sept. 3, 2022), https://blog.cloudflare.com/kiwifarms-blocked/.
[71] Mathew Ingram, *Platform Ban of Trump and Parler Raises Questions about Speech and Power*, Columbia Journalism Review (Jan. 14, 2021).
[72] Ronan Fahy, Judith Möller & Rocco Bellanova, *Deplatforming Politicians and the Implications for Europe*, Digit. Legal Lab (Feb. 2021), https://www.sectorplandls.nl/wordpress/blog/deplatforming-politicians-and-the-implications-for-europe/.
[73] Pablo Chavez, *Toward Digital Solidarity*, Lawfare (June 28, 2022, 10:01 AM), https://www.lawfaremedia.org/article/toward-digital-solidarity.
[74] Aruna Viswanatha, *FBI's Christopher Wray Wants Business to Help Fight China, Cyber Threats*, Wall St. J. (Feb. 9, 2023, 9:48 AM), https://www.wsj.com/articles/christopher-wray-tries-to-thaw-fbis-frosty-relationship-with-business-11675911906?mod=Searchresults_pos4&page=1.

laws"[75] (including, presumably, the concurrent application of U.S. domestic law for law enforcement and national security purposes).

But the same EU-based cloud service providers that would benefit, in the name of security, from these commercially protectionist arrangements have global aspirations. And once they operate outside the EU, including in the United States—as several of them already do—these providers become subject to U.S. jurisdiction and therefore to valid U.S. government requests for data, just like U.S.-based providers are. In any event, these sovereignty-based policies are often rooted in a profound misunderstanding of U.S. law enforcement's ability to access such data when stored by U.S.-based service providers. Some European officials have pointed to a 2018 U.S. law called the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[76] (described further below) as a principal reason why their nations should move away from cloud solutions offered by non-EU companies and instead should deploy European-designed cloud solutions. In fact, U.S. law in this area is consistent with international principles, and it affords very high privacy protections—including protections that are more rigorous than what domestic governments in Europe typically provide to their own citizens.

SecNumCloud and French Digital Sovereignty

Recent developments in France demonstrate the drawbacks of a sovereignty-based approach. The French national cybersecurity agency, known as ANSSI,[77] launched the SecNumCloud certification scheme in 2016 in an effort to improve information security for French government agencies and firms that operate in critical sectors and qualify as operators of vital importance[78] (OVIs). All OVIs must use SecNumCloud-certified cloud services. The SecNumCloud label is granted to service offerings that fulfill a set of requirements based on the internationally recognized ISO 27001[79] standard. Many of those requirements,[80] including "physical access controls, strong authentication with password hashing and salting, [and] software encryption," among others, reflect familiar cybersecurity best practices and procedures. To date, the service

[75] Laurens Cerulus, *France wants cyber rule to curb US access to EU data*, POLITICO (Sept. 13, 2021, 5:23 PM), https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/.
[76] Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2523.
[77] ANSSI, *Agence nationale de la sécurité des systèmes d'information* [French National Agency for the Security of Information Systems], ANSSI, https://www.ssi.gouv.fr/en/ (last visited Aug 24, 2023).
[78] Chakib Kissane, *Sécurité des systèmes d'information des OIV: une législation stricte pour protéger les entreprises stratégiques* [Security of OIV information systems: strict legislation to protect strategic companies], OODRIVE: REGULATION BLOG (Aug. 24, 2023), https://www.oodrive.com/blog/security/secnumcloud-the-certification-for-cloud-confidence-service-providers/.
[79] INT'L ORG. FOR STANDARDIZATION, ISO/IEC 27001: Information Security Management Systems, https://www.iso.org/standard/27001 (last visited Aug. 23, 2023).
[80] Chakib Kissane, *SecNumCloud: the Certification for Cloud Confidence Service Providers*, OODRIVE: SECURITY BLOG (Aug 24, 2023), https://www.oodrive.com/blog/security/secnumcloud-the-certification-for-cloud-confidence-service-providers/.

offerings of only a handful of firms,[81] all of them French, have been granted the SecNumCloud label.

ANSSI periodically refines the SecNumCloud requirements, and it is the revision[82] proposed in September 2021 (English translation here),[83] which went into effect[84] in March 2022,[85] that is particularly concerning. This revision is expressly protectionist and, consistent with the French national cloud strategy[86] published in 2021, imposes a number of controversial, "sovereignty"-based conditions that ironically could endanger the security of French critical-sector information. As one commentator has observed,[87] the revision includes

severe, China-like restrictions that force foreign firms to store data locally and only use local support and technical staff …. Similar to China, it would effectively only allow local firms to attempt for certification, and thus force foreign firms to set up a local joint venture to try to be certified as "trusted." ... [The revision would] disadvantage—and effectively preclude—foreign cloud firms from providing services to government agencies as well as 600-plus firms that operate "vital" and "essential" services.

The revision also contains an entire newly drafted provision, Section 19.6,[88] which requires certified cloud service providers to have "immunity to non-EU laws" ["protection vis-à-vis du droit extra-européen"]. As discussed below, that provision in particular is self-defeating.

If the latest SecNumCloud revision represents "digital sovereignty," then the concept is deeply flawed. The costs of data localization, writ large, are well known. Digital flows exert a greater

---

[81] ANSSI, *Liste des produits et services qualifies* [List of qualified products and services], ANSSI, https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf (last visited Aug 23, 2023).
[82] ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences*, [Cloud Service Providers (SecNumCloud) Requirements repository], ANSSI (Sept. 21, 2021), https://www.ssi.gouv.fr/uploads/2021/10/anssi-referentiel_exigences-secnumcloud-v3.2.a.pdf.
[83] INFO. TECH. & INNOVATION FOUND., *SecNumCloud 3.2.a*, INFO. TECH. & INNOVATION FOUND. (2021), https://www2.itif.org/2021-secnumcloud-3.2.a-english-version.pdf?_ga=2.99563933.2054818016.1642970070-1088519388.1642472569.
[84] ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences* [Cloud Service Providers (SecNumCloud) Requirements repository] (Mar. 8, 2022), https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf.
[85] DATAGUIDANCE, *France: ANSSI Updates Certification Framework for Cloud Service Providers to Account for* Schrems II *Requirements, Endorsed by CNIL*, DATAGUIDANCE (Mar. 11, 2022), https://www.dataguidance.com/news/france-anssi-updates-certification-framework-cloud.
[86] Press Release, Direction interministérielle du numérique [Interministerial Digital Directorate], *Le gouvernement annonce sa stratégie nationale pour le Cloud* [Government Announces National Cloud Strategy] (May 17, 2021), https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-nationale-pour-le-cloud/.
[87] Nigel Cory, *"Sovereignty Requirements" in France—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners*, CROSS-BORDER DATA FORUM (Dec. 10, 2021), https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/.
[88] ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences*, [Cloud Service Providers (SecNumCloud) Requirements repository], ANSSI (Sept. 21, 2021), https://www.ssi.gouv.fr/uploads/2021/10/anssi-referentiel_exigences-secnumcloud-v3.2.a_revision.pdf.

impact[89] over economic growth than traditional goods. It follows that cross-border data restrictions significantly impact GDP.[90] Forced localization also reduces domestic investment[91] and economic welfare[92] and could result in the "tangible degradation[93] or loss of many digital services and business functionalities that rely on cross-border data flows." But the costs associated with data protectionism are not just economic. Such protectionism also threatens scientific and technological advancement, particularly in areas like data science[94] and the "Internet of Things."[95] In addition, fragmentation and localization of internet communication promotes censorship and surveillance, thereby increasing the ability of malign actors to target free expression[96] and infringe on human rights.

Linking data localization requirements to purported cybersecurity benefits is especially problematic. As one prominent trade association has observed,[97] "How data is protected is much more important to security than where it is stored." In fact, the latest SecNumCloud revision's mandate that all OVIs must store and process data within certain territorial limits raises significant cybersecurity red flags. For instance, increased data localization translates to an increase in the number of data centers,[98] as providers are forced to maintain a physical presence in every country in which they seek to do business, rather than consolidating their operations into a limited number of fortified data centers located strategically around the globe. More data centers mean more staffing, with the associated increases in the risk of human compromise and human error; more data centers also translate to more potential points of hardware and software compromise. Thus, ironically, localization can create a larger and more vulnerable surface area, while providing malign actors with a set of concrete, identifiable targets on which to focus both cyberattacks and physical attacks. (This is precisely why, for example, Ukrainian officials, in the days before the Russian invasion, "transfer[ed] the existing local servers [containing government

---

[89] *See* James Manyika ET AL., *Digital Globalization: The New Era of Global Flows*, MCKINSEY GLOBAL INSTITUTE (Feb. 24, 2016), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows (noting that now "digital flows . . . exert a larger impact on GDP growth than the centuries-old trade in goods").
[90] *See* Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, INFO. TECH. & INNOVATION FOUND. (July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/#_edn6 (presenting regression data indicating a correlation between unrestricting data flows and higher gross domestic product).
[91] Asia Internet Coalition, ASIA INTERNET COALITION, https://aicasia.org/ (last visited Aug. 23, 2023).
[92] Emily Wu, *Sovereignty and Data Localization*, HARVARD KENNEDY SCH.: BELFER CTR FOR SCI. AND INT'L AFF'S (July 2021).
[93] CTR. FOR INFO. POL'Y LEADERSHIP AND TECH, LAW & SEC. PROG., THE "REAL LIFE HARMS" OF DATA LOCALIZATION POLICIES: DISCUSSION PAPER 1, CTR. FOR INFO. POL'Y LEADERSHIP (Mar. 2023).
[94] Helena U. Vrabec ET AL., HANDBOOK ON DATA SCIENCE AND LAW: DATA LOCALISATION MEASURES AND THEIR IMPACTS ON DATA SCIENCE, 13 (2018).
[95] Hosuk Lee-Makiyama and Simon Lacy, CROSS-BORDER DATA FLOWS: THE IMPACT OF DATA LOCALISATION ON IOT, GLOB. SYS. FOR MOBILE COMMC'NS ASS'N (Jan. 18, 2021), https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf.
[96] Erol Yayboke ET AL., THE REAL NATIONAL SECURITY CONCERNS OVER DATA LOCALIZATION, CTR. FOR STRATEGIC AND INT'L STUD. (July 23, 2021).
[97] BUS. SOFTWARE ALL., THE SOFTWARE ALLIANCE'S COMMENTS TO ANSSI ON SECNUMCLOUD (Version 3.2.A), BUS. SOFTWARE ALL., (Nov. 2021).
[98] Erol Yayboke ET AL., THE REAL NATIONAL SECURITY CONCERNS OVER DATA LOCALIZATION, CTR. FOR STRATEGIC AND INT'L STUD. (July 23, 2021).

data] to the public cloud,"[99] effectively "evacuat[ing] critical government data" to processing centers located outside the country.)

In addition, the notion that maintaining an entity's entire technology "stack"[100] in one physical place is the best way "to generate the required level of trust in certified cloud services" is simply wrong.[101] Most unauthorized intrusions into computer networks are accomplished remotely, so physically consolidating the relevant people, hardware, software, and infrastructure in territorial space accomplishes very little in terms of cyber defense. Moreover, requirements to use local support and technical staff create additional redundancies and associated points of compromise; and to the extent those staff members may lack best-in-class knowledge and training, their presence could well prove counterproductive.

On a broader scale, data localization inhibits cybersecurity advances by reducing the overall amount of cyber-threat information available to governments, businesses, and researchers. As commentators have observed,[102]

The accelerating arms race in cyber warfare requires increasingly sophisticated and constantly evolving defense solutions. Public cloud service providers and cloud based cyber security firms have delivered incredibly valuable common solutions where the economies of scale, access to scarce talent resources, and the ability to monitor global networks in real time have provided an essential solution to enterprises trying to cope and to regulatory supervisors looking for workable solutions.

To say this is not to deny the cloud's unique vulnerabilities.[103] But by interrupting the critically important pooling of real-time cyberthreat information, data localization weakens common global defenses. Imposing strict sovereignty controls also significantly reduces consumer choice, as few providers will be able to meet the relevant requirements, and those that do may nonetheless reflect "shortcomings"[104] when compared to global best-in-class offerings. Such

---

[99] Microsoft, *CEE Multi-Country News Center: How technology helped Ukraine resist during wartime*, Microsoft (Jan. 20, 2023), https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/.
[100] Yann Lechelle, *It is Time to Strengthen our EU Data Sovereignty - Open Letter to EU Institutions*, LinkedIn (Mar. 23, 2021), https://www.linkedin.com/pulse/time-strengthen-our-eu-data-sovereignty-open-letter-yann-lechelle/.
[101] *See* Nigel Cory, *"Sovereignty Requirements" in France—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners*, Cross-Border Data Forum (Dec. 10, 2021), https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/ (arguing that such an approach leads to a "false sense of security").
[102] Conan French et al., *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy*, at 6-7, Inst. of Int'l Fin. (Dec. 2020), https://www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf (noting that data localization "undermine[s]" cybersecurity and also "weaken[s] common global defenses").
[103] John Sakellariadis, *Biden admin's cloud security problem: 'It could take down the internet like a stack of dominos'*, Politico (Mar. 10, 2023, 3:12 PM), https://www.politico.com/news/2023/03/10/white-house-cloud-overhaul-00086595.
[104] Letter from Angela Merkel, Chancellor of Germany, et al., to Ursula von der Leyen, President, Eur. Comm'n. (Mar. 1, 2021).

controls thus "make[] the ecosystem less diversified"[105] and once again "more vulnerable to attacks."[106]

The ENISA/EUCS Framework

If recent developments on the SecNumCloud front were not concerning enough, the French government has been working to extend the sovereignty-based approach on an EU-wide scale. Indeed, France[107] has been advocating[108] for the European Union Agency for Cybersecurity (ENISA) to include sovereignty requirements[109] identical to SecNumCloud in that agency's cloud service initiative, the EU Cloud Security Scheme (EUCS).[110] Efforts to finalize the EUCS requirements are currently accelerating. A high-level working group is understood to have met on May 26[111] to discuss the latest draft version[112] of the scheme, which could be finalized within the next few months[113] and in its current form contains several "hard" sovereignty requirements.

By way of background: The EU has enacted a number of initiatives over the past few years designed to enhance Europe's cybersecurity posture, including the Network and Information Security Directive[114] (the NIS Directive), the Cybersecurity Act,[115] and the EU cybersecurity certification framework.[116] The NIS Directive, adopted in 2016, was the first piece of EU-wide cybersecurity legislation. Recently updated (NIS2),[117] the directive required member states to

---

[105] Letter from Guido Lobrano, Vice President and Dir. Gen. for Europe, Info. Tech. Indust. Counc., to the French National Agency for the Security of Information Systems (Dec. 8, 2021).
[106] *Id*.
[107] Nigel Cory, *"Sovereignty Requirements" in French—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners*, Info. Tech. & Innovation Found. (Dec. 10, 2021), https://itif.org/publications/2021/12/10/sovereignty-requirements-france-and-potentially-eu-cybersecurity/.
[108] Nigel Cory, *"Sovereignty Requirements" in France—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners*, Cross-Border Data Forum (Dec. 10, 2021), https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/.
[109] Laurens Cerulus, *France wants cyber rule to curb US access to EU data*, Politico (Sept. 13, 2021), https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/.
[110] European Union Agency for Cybersecurity Press Release, Cloud Certification Scheme: Building Trusted Cloud Services Across Europe (Dec. 22, 2020).
[111] Lucca Bertuzzi, *EU Cloud Certification Headed for Tiered Approach on Sovereignty Criteria*, Euractiv (May 12, 2023), https://www.euractiv.com/section/cybersecurity/news/eu-cloud-certification-headed-for-tiered-approach-on-sovereignty-criteria/.
[112] Eur. Union Agency for Cybersecurity, *Draft Version of EUCS – Cloud Services Scheme V1.0.319*, Eur. Union Agency for Cybersecurity (May 2023).
[113] Matthias Bauer, Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements, European Centre for International Political Economy (March 2023).
[114] Eur. Union Agency for Cybersecurity, *NIS Directive*, Eur. Union Agency for Cybersecurity, (2023), https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new (last visited Aug. 16, 2023).
[115] Eur. Comm'n, *The EU Cybersecurity Act*, Eur. Comm'n (Apr. 18, 2023), https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.
[116] Eur. Union Agency for Cybersecurity, *Certification*, European Union Agency for Cybersecurity, Eur. Comm'n (last visited Aug. 16, 2023), https://www.enisa.europa.eu/topics/standards/certification.
[117] Eur. Comm'n, *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive),* Eur. Comm'n, (Jan. 16, 2023).

craft national cybersecurity standards, to collaborate with other EU countries in the development and maintenance of cross-border networks, and to supervise critical sectors. Subsequent directives have strengthened ENISA's authority. The Cybersecurity Act, for example, permanently extends ENISA's mandate[118] to achieve "a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity." Under the authority of the Cybersecurity Act, ENISA adopted the certification framework,[119] which establishes EU-wide certification schemes for the information and communication technology sector.

To continue its push toward EU-wide cybersecurity regulation, ENISA released the first public draft of the EUCS[120] in late 2020. The plan establishes three security assurance levels: basic, substantial, and high. And while "it has been argued"[121] that the EUCS high assurance level is "only meant to address 'state-confidential' scenarios," this assurance level is in fact "much broader in scope" in its "potential market and broader economic impact." As commentators have observed,[122] under Article 52(7) of the Cybersecurity Act,[123] "level high is the only level intended to 'minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources.' This will make level 'high' the go-to choice for cloud [solutions in Europe], particularly considering that the GDPR requires due consideration for the 'state of the art' for security." Meanwhile, though EUCS certification itself is voluntary, customers—whether governmental or commercial—are free to include it as a mandatory tender requirement.[124] In addition, "NIS2 allows EU governments[125] and the European Commission to mandate certain cloud customers to only use a certified EUCS cloud service," which may well become the case "for the numerous[126] entities deemed essential or important" under the updated directive.

The insertion of SecNumCloud-like "sovereignty" requirements into the EUCS high assurance level would therefore be hugely significant. And that is precisely what the European Commission apparently asked ENISA to do[127] in early 2022, during the French presidency of the EU. "The

---

[118] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No. 526/2013 (Cybersecurity Act), 2019 O.J. (L 151).
[119] Eur. Union Agency for Cybersecurity, *Certification*, European Union Agency for Cybersecurity, Eur. Comm'n (last visited Aug. 16, 2023), https://www.enisa.europa.eu/topics/standards/certification.
[120] Eur. Union Agency for Cybersecurity, *Draft Version of the Cloud Services Scheme*, Eur. Union Agency for Cybersecurity (May 2023).
[121] Cecilia Bonefeld-Dahl, Data Transfers in the Data Strategy: Understanding Myth and Reality, DigitalEurope (June 16, 2022).
[122] *Id*.
[123] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No. 526/2013 (Cybersecurity Act), 2019 O.J. (L 151) 57.
[124] Matthias Bauer, Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements, European Centre for International Political Economy (March 2023).
[125] *Id*.
[126] Lucca Bertuzzi, *EU Cloud Certification Headed for Tiered Approach on Sovereignty Criteria*, Euractiv (May 12, 2023), https://www.euractiv.com/section/cybersecurity/news/eu-cloud-certification-headed-for-tiered-approach-on-sovereignty-criteria/.
[127] Laura Kabelka, *Sovereignty Requirements Remain in Cloud Certification Scheme Despite Backlash*, Euractiv (June 21, 2022),

drafting of EUCS has been criticized for a lack of transparency and accountability,"[128] and the exact contents of the scheme's proposed "Annex J" ("Protection of European Data Against Unlawful Access")[129] were long shrouded in secrecy and speculation until they were released (via media leak) just a few days ago. I discuss those draft requirements in the next section. As a general matter, ENISA has proposed adding requirements[130] designed[131] to "ensure immunity from foreign jurisdictions" and to diminish foreign participation in the European cloud market. For the reasons described above, such a framework would actually weaken Europe's overall cybersecurity posture.

Such a framework would also contrast starkly[132] with public-sector cybersecurity standards adopted in other parts of the free world. In the United States, for example, FedRAMP[133] authorizes cloud service offerings to the federal government at various "impact"[134] levels (low, moderate, and high), depending on the security objective. While individual U.S. agencies may impose citizenship or data handling conditions in connection with particular programs or projects, FedRAMP itself imposes no citizenship[135] or data localization requirements. It follows that the list of FedRAMP-certified products[136] contains the cloud service offerings of many non-U.S.-based firms, including several at the high level.[137] This is as it should be: Cybersecurity standards should actually promote cybersecurity, rather than advance narrow political or commercial agendas. Considering the outsized role[138] that European standard-setting plays in global technology matters, this is an area in which European policymakers need to display true international leadership.

Misunderstanding the CLOUD Act

---

https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash/.

[128] Georgia Wood and James Andrew Lewis, *The CLOUD Act and Transatlantic Trust*, Ctr. for Strategic and Int'l Stud. (Mar. 29, 2023), https://www.csis.org/analysis/cloud-act-and-transatlantic-trust.

[129] Eur. Union Agency for Cybersecurity, *Draft Version of the Cloud Services Scheme*, Eur. Union Agency for Cybersecurity (May 2023).

[130] *See* Online Trust Coalition, Non-paper by DE, ES, FR and IT on the EUCS Requirements for Immunity to Non-EU Laws, (2021) (proposing revisions to the European Union Cloud Services Scheme, or "EUCS").

[131] Matthias Bauer, Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements, 3, European Centre for International Political Economy (March 2023).

[132] Nigel Cory, *Europe's Cloud Security Regime Should Focus on Technology, Not Nationality*, Info. Tech. & Innovation Found. (Mar. 27, 2023), https://itif.org/publications/2023/03/27/europes-cloud-security-regime-should-focus-on-technology-not-nationality/.

[133] Fed. Risk and Authorization Mgmt. Program, *Federal Risk and Authorization Management Program: Program Basics*, Gen. Servs. Admin., https://www.fedramp.gov/program-basics/.

[134] Fed. Risk and Authorization Mgmt. Program, *Understanding Baselines and Impact Levels in FedRAMP*, FedRAMP Blog (Nov. 16, 2017), https://www.fedramp.gov/understanding-baselines-and-impact-levels/.

[135] FedRamp Comment to Question: Citizenship #130, GitHub (Jun. 11, 2017), https://github.com/GSA/fedramp-tailored/issues/130#issuecomment-314425577.

[136] ed. Risk and Authorization Mgmt. Program, *Federal Risk and Authorization Management Program: FedRAMP Marketplace*, Gen. Servs. Admin., https://marketplace.fedramp.gov/products.

[137] Matthias Bauer, Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements, European Centre for International Political Economy (March 2023).

[138] *See generally* Anu Bradford, The Brussels Effect: How the European Union Rules the World, (2020) (offering that the European Union holds a relatively large amount of general geopolitical influence).

One of the principal motivations behind Europe's push for "digital strategic autonomy"[139] is the idea that allowing non-European cloud providers to store sensitive European data would afford foreign nations—in particular the United States—inappropriate, or least undesired, access to that data, including potentially for commercial advantage. (Despite widespread recognition[140] in Europe that "substantial protection of personal data against government access does not exist in [for example] the PRC," when European digital sovereigntists refer to "non-EU law," they typically[141] focus[142] on the United States—though recent news[143] may indicate early signs of a possible shift in attitude.)

As early as 2015, the French government voiced its concerns[144] about OVIs' use "of applications and data processing hosted in uncontrolled virtual spaces, supported by physical infrastructures located outside the national territory and not subject to European law." More recently, the European Commission has advanced the notion[145] that because "data produced in Europe is generally stored and processed outside Europe," this "bring[s] risks in terms of cybersecurity ... [and of] unlawful access to data by third countries." A prominent EU commissioner echoed this view[146] when he declared that "[o]ur digital sovereignty rests [in part] on ... control over our data …. [I]t is becoming imperative to have autonomous European clouds that guarantee our companies that their industrial data will not be subject to any third country law and will be protected against external cyber interference." Under this reasoning, the obvious solution should be to require such data to be stored and processed in Europe, where presumably it would remain outside the grasp of non-EU government officials.

In advancing such arguments regarding the need for "immunity to non-EU laws," European government officials[147] and industry leaders[148] have often relied on a flawed reading of the

---

[139] Charles Michel, President, Eur. Counc., Speech at Masters of Digital 2021: Digital sovereignty is central to European strategic autonomy (Feb. 3, 2021) (articulating "strategic autonomy" as "mean[ing] more resilience, more influence[] [a]nd less dependence").
[140] Milieu Consulting, Final Report EDPS/2019/02-13: Government Access to Data in Third Countries, Milieu Consulting (Nov. 2021).
[141] Evelyn Chang and Ryan Browne, *Europe's Crackdown on Big Tech Omitted TikTok – but now that's set to Change*, CNBC (Jan. 30, 2023), https://www.cnbc.com/2023/01/30/tiktok-in-europes-crosshairs-as-us-mulls-ban-on-chinese-owned-app.html.
[142] Rahiel Nasir, OVHcloud: *Putting the Final Pieces in Place for Europe's Digital Fortress?,* OVHCloud (Nov. 19, 2021), https://corporate.ovhcloud.com/sites/default/files/2021-12/idc-ovhcloud-putting-the-final-pieces-in-place-for-europes-digital-fortress-2021-nov.pdf.
[143] *See* Supantha Mukherjee, *Comply with EU Rules or Face Ban, Breton Tells TikTok CEO*, Reuters (Jan. 19, 2023), https://www.reuters.com/technology/comply-with-eu-rules-or-face-ban-breton-tells-tiktok-ceo-2023-01-19/ (noting a firm warning from European Commissioner Thierry Breton to the CEO of TikTok that the company may be banned in the European Union over failing to comply with new EU data protection standards).
[144] French National Digital Security Strategy (Oct. 16, 2015).
[145] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2030 Digital Compass: the European Way for the Digital Decade*, COM (2021) 118 final (Mar. 9, 2021).
[146] Thierry Breton, *Europe: The Keys to Sovereignty*, LinkedIn (Sept. 11, 2020), https://www.linkedin.com/pulse/europe-keys-sovereignty-thierry-breton.
[147] Laurens Cerulus, *France wants cyber rule to curb US access to EU data*, Politico (Sept. 13, 2021, 5:23 PM), https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/.
[148] Bitkom, Key Points: A Sovereign Cloud and Data Infrastructure for Germany and Europe, Bitkom (Nov. 15, 2019).

CLOUD Act[149] a Trump-era statute that clarifies the legal framework for U.S. law enforcement requests for data that is held by telecommunications service providers. Many Europeans think[150] that the CLOUD Act allows U.S. law enforcement agencies free access to data stored anywhere in the cloud by U.S.-based CSPs. European critics[151] of the CLOUD Act believe that the statute permits U.S. law enforcement officials to arbitrarily access EU person data, even when that data is stored in a data center located in Europe, so long as the CSP itself is headquartered in the United States.

This understanding is mistaken on multiple levels.

First, the CLOUD Act does not discriminate based on nationality. The statute applies to any communications service provider[152] subject to U.S. jurisdiction, including those based in the EU. Recall that service offerings of only five CSPs (all of them French) have been certified under the SecNumCloud scheme and are considered "trusted" under French domestic cybersecurity standards. At least three of those firms (3DS Outscale,[153] OVH,[154] and WorldLine Cloud Services)[155] do business in the United States, are therefore subject to the CLOUD Act, and accordingly are not "immune to non-EU laws." (A fourth, Cloud Temple, also maintains offices outside of Europe.)[156] To the extent the sovereignty-based approach vastly privileges large EU-based cloud service providers[157] (that have global ambitions) over smaller ones, it is difficult to see how those EU-based providers could satisfy the requirement of being "immune to non-EU laws."

Second, the CLOUD Act requires service providers,[158] when served with appropriate legal process, to disclose to the U.S. government relevant information "within such provider's possession, custody, or control," regardless of whether such information "is located within or outside the United States." This language makes explicit in U.S. law the long-established international law principle that any company subject to a particular country's jurisdiction can be required to produce data the company controls, regardless of where the data is stored at any point

---

[149] Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2523.
[150] *See* European Parliament Memorandum PE 651.992, Digital Sovereignty for Europe (July 2020) (cautioning against an "expansive extra-territorial ability granted to US law enforcement agencies to obtain foreigners' personal data under the 2018 US CLOUD Act").
[151] *See* Laurens Cerulus, *France wants cyber rule to curb US access to EU data*, POLITICO (Sept. 13, 2021, 5:23 PM), https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/ (declaring a need to prevent non-European law applying to European digital services).
[152] *Id*.
[153] OUTSCALE, *Secure, Scalable, and Compliant IaaS Solutions Built for the Most Demanding Requirements*, OUTSCALE, (2023), https://us.outscale.com/ (last visited Aug. 12, 2023).
[154] OVHCLOUD, *OVHcloud Products and Solutions for Your Business*, OVHCLOUD (2023), https://us.ovhcloud.com/ (last visited Aug. 12, 2023).
[155] WORLDLINE, *Payments Technology Designed to Help You Grow*, WORLDLINE (2023), https://worldline.com/en/home/about-us.html (last visited Aug. 12, 2023).
[156] CLOUD TEMPLE, Africa, CLOUD TEMPLE (2023), https://www.cloud-temple.com/en/region/africa/ (last visited Aug. 14, 2023).
[157] Mathieu Pollet, *French Cloud Industry Regrets Government's Ambivalence in Dealing with Digital Giants*, EURACTIV (Oct. 22, 2021), https://www.euractiv.com/section/digital/news/french-cloud-industry-regrets-governments-ambivalence-in-dealing-with-digital-giants/.
[158] 18 U.S.C. § 2713.

in time. This principle is certainly not unique to U.S. law;[159] French courts, for example, have long permitted[160] French law enforcement to obtain data located outside that nation so long as it is retrievable from a computer located in France. In fact, the power under domestic law to compel production of data that is within a provider's "possession or control,"[161] irrespective of where the data happens to be stored, is a requirement of the Budapest Convention on Cybercrime, which over 65 nations—including nearly every EU member state—have ratified. Notably, the same principle undergirds both the recent OECD declaration[162] and the EU's newly enacted e-evidence regulation[163] ("application of this Regulation should not depend on the actual location of the service provider's establishment or of the data processing or storage facility"). Of course, if the relevant information is stored outside of the "possession, custody, or control" of the entity that U.S. law enforcement serves with legal process, then that marks the end of the inquiry.

Third, the notion that U.S. law enforcement can capriciously access the content of sensitive EU data stored by U.S.-based providers is simply false. Again, U.S. law in this context does not discriminate based on nationality. In order to gain access to the contents of any person's stored communications data through service of process on any CSP within its jurisdiction (without notifying the user), U.S. law enforcement must secure a warrant. The warrant must meet demanding, privacy-protective U.S. constitutional requirements.[164] For instance, the warrant must be supported by an affidavit sworn under penalty of perjury showing probable cause that the place searched will contain particular things subject to seizure. This affidavit, in turn, must state with particularity the crime that is alleged, the information to be disclosed, and the evidence to be seized. The warrant package as a whole must then be submitted to, and approved by, an independent judge. Thus, when U.S. law enforcement accesses the contents of, say, a French citizen's emails stored by a U.S.-based cloud service provider, not only must the government satisfy the same standards used to access a U.S. citizen's data, but that showing is more rigorous[165] than what the French government would have to make to access that same person's data if it were stored with a SecNumCloud-certified provider.

Fourth, the CLOUD Act itself recognizes the need for CSPs to protect the confidentiality of their customers' data and creates mechanisms for providers to do just that. For example, the statute recognizes procedures[166] that allow CSPs subject to U.S. jurisdiction, irrespective of where they

---

[159] Shanzay Pervais & Alex Joel, Data Localization and Government Access to Data Stored Abroad: Discussion Paper 2, Technology, Law and Security: Privacy Across Borders (Mar. 29, 2023).
[160] Michael Punke, *AWS and the CLOUD Act*, AWS Security Blog (May 27, 2019), https://aws.amazon.com/blogs/security/aws-and-the-cloud-act/.
[161] Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185.
[162] Org. for Econ. Co-operation and Dev., *Declaration on Government Access to Personal Data Held by Private Sector Entities*, Org. for Econ. Co-operation and Dev. (Dec. 13 2022), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.
[163] Council of the European Union Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM (2018) 225 (Jan. 20, 2023).
[164] Off. Int'l Affr's, A Brief Explanation of Probable Cause for Foreign Authorities, U.S. Dep't Just. (Apr. 2022).
[165] Mark Scott & Clothilde Goujard, *US to EU: We want to check your surveillance practices*, Politico (Apr. 27, 2023), https://www.politico.eu/article/washington-to-brussels-we-want-to-check-your-surveillance-practices/.
[166] *See* 18 U.S.C. § 2703(h)(2) (providing for certain circumstances when an electronic communication service provider may file a motion to quash such a demand).

are headquartered, to challenge certain U.S. government data demands in court. Where, for instance, a U.S. government request conflicts with another country's laws (like the GDPR), the CLOUD Act recognizes the right of the provider[167] to challenge that request on traditional conflict of law principles. In addition, the statute is encryption neutral, which means that CSPs remain free to provide their customers with encryption services that render the data they store unintelligible to the provider. This, of course, has obvious implications for U.S. law enforcement's ability to access that data through service of process on the provider.

Fifth, U.S. law enforcement and national security officials do not seek access to "industrial data" in order to pursue U.S. commercial advantage. Data can be secured under the relevant legal authorities, including the CLOUD Act, only for authorized public safety purposes, and there are significant[168] penalties[169] for its misuse. Even as the U.S. Department of Justice forges[170] closer[171] collaboration[172] with "economic" agencies like the U.S. Department of the Treasury and the U.S. Department of Commerce—and even as those agencies seek information from foreign firms[173] and deploy novel[174] enforcement capabilities[175] of their own—the relevant data would not be shared[176] with the U.S. private sector to advance national economic or commercial goals. Other

[167] 18 U.S.C. § 2703(h)(2)(ii).
[168] *See* 18 U.S.C. § 2707(c) (allowing a court to award punitive damages including "any profits made by [a] violator").
[169] *See* 18 U.S.C. § 1832(b) (permitting a maximum financial penalty of either $5,000,000 or three times the amount of the stolen trade secret's value).
[170] Press Release, U.S. Dep't Treasury, *U.S. Departments of Treasury and Justice Launch Multilateral Russian Oligarch Task Force*, U.S. Dep't Treasury (Mar. 16, 2022), https://home.treasury.gov/news/press-releases/jy0659.
[171] Press Release, Off. Pub. Affr's, *Departments of Justice, Commerce and Treasury Issue Joint Compliance Note on Russia-Related Sanctions Evasion and Export Controls*, U.S. Dep't Just. (Mar. 2, 2023), https://www.justice.gov/opa/pr/departments-justice-commerce-and-treasury-issue-joint-compliance-note-russia-related.
[172] Press Release, Off. Pub. Affr's, *Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force*, U.S. Dep't Just. (Feb. 16, 2023), https://www.justice.gov/opa/pr/justice-and-commerce-departments-announce-creation-disruptive-technology-strike-force.
[173] Press Release, Gina M. Raimondo, *U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order*, U.S. Dep't. Com. (Mar. 17, 2021), https://www.commerce.gov/news/press-releases/2021/03/us-secretary-commerce-gina-raimondo-statement-actions-taken-under-icts.
[174] Press Release, Wally Adeyemo, *Remarks by Deputy Secretary of the Treasury Wally Adeyemo on Action Against Russian Illicit Finance*, U.S. Dep't Treasury (Jan. 18, 2023), https://home.treasury.gov/news/press-releases/jy1193.
[175] U.S. Dep't. Com., Export Enforcement: 2022 Year in Review, U.S. Dep't. Com. (Jan. 04, 2023).
[176] Justin Hemmings & Nathan Swire, *The Cloud Act Is Not a Tool for Theft of Trade Secrets*, Lawfare Blog (Apr. 23, 2019, 8:00 AM), https://www.lawfaremedia.org/article/cloud-act-not-tool-theft-trade-secrets.

nations[177] may regard economic[178] espionage[179] differently[180], but such are the rules and norms[181] in the United States.

Finally, U.S. federal law enforcement has adopted a policy[182] stating that when prosecutors seek information that an entity has stored with a CSP, they "should seek [that] data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation." One would expect U.S. authorities to seek access to sensitive EU public-sector data in connection with only the most significant law enforcement investigations and only then after robust internal (and possibly interagency) discussion. Even at that point, the policy seems to require U.S. law enforcement, in all but the most exceptional cases, to seek the data directly from the relevant EU-based public-sector agency—an action that itself would surely be prefaced by extensive intergovernmental discussion and negotiation and would likely fall outside the scope of the CLOUD Act entirely.

The Path Ahead

This is a pivotal moment in the future of international data flows, as two competing visions of digital sovereignty continue jostling for primacy. The first vision recognizes the critical importance of the free flow of information across borders (at least among rule-of-law nations) for commercial innovation. And it acknowledges the need for government actors to efficiently access data stored outside their borders in order to advance domestic sovereign interests in public safety—even as it insists on robust baseline individual privacy and civil liberties protections and respects sovereign differences.

By contrast, the second vision promotes a nationality- and territory-based conception of data security and trust. That vision is not only deeply suspicious of cross-border jurisdictional claims and enforcement but also brazenly dismissive of other nations' sovereign interests. Its most extreme adherents harbor citizens who commit crimes under foreign law[183], while unilaterally

---

[177] *See* Christopher Dickey, *Parlez-Vous Espionage?*, Newsweek (Sept. 22, 1991, 8:00 AM), https://www.newsweek.com/parlez-vous-espionage-203426 (describing an investigative report of a French espionage attempt against American business executives to provide an advantage to French businesses).
[178] Daniel Liberto, *Economic Espionage*, Investopedia (Nov. 30, 2021), https://www.investopedia.com/terms/e/economic-espionage.asp.
[179] Nat'l Counterintelligence and Cybersecurity Ctr., Foreign Economic Espionage in Cyberspace: 2018, Nat'l Counterintelligence and Cybersecurity Ctr. (2018).
[180] Yudhijit Bhattacharjee, *The Daring Ruse That Exposed China's Campaign to Steal American Secrets*, N.Y. Times (Mar. 7, 2023), https://www.nytimes.com/2023/03/07/magazine/china-spying-intellectual-property.html.
[181] Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 7, 2022).
[182] Comput. Crime and Intell. Prop. Section, Seeking Enterprise Customer Data Held by Cloud Service Providers, U.S. Dep't Just. (Dec. 2017).
[183] Frank Bajak, *How the Kremlin provides a safe harbor for ransomware*, Assoc. Press (Apr. 16, 2021, 5:15 PM), https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999.

hunting[184] down[185] those citizens abroad whose alleged domestic crimes have gone unpunished. Advanced in international fora by nations like Russia[186] and China,[187] this vision endorses the view that governments should tightly control data concerning their citizens (and, increasingly, their economies)[188] within their borders, even while (as the Chinese example[189] makes clear) they freely collect and wield data concerning citizens of other nations for "geopolitical"[190] and related purposes.[191]

In Europe, the struggle between these two visions is playing out before our eyes. To be sure, the sovereignty-based approach differs in important ways from the Russian and Chinese models; as commentators have observed,[192] "[T]he EU version of digital sovereignty does not give governments privileged access to technology and data, nor reinforce regime control over the digital economy." But in broad outlines, the similarities are undeniable—and the fervor of the internal debates over the EUCS confirms the enormity of the stakes.

Indeed, several EU member states[193] have departed from the French position[194] and have voiced their concerns over the scheme's autarkic turn. The governments of Denmark, Estonia, Greece, Ireland, the Netherlands, Poland, and Sweden observe in a non-paper submitted to the Council of

---

[184] Jorge González-Gallarza, *Why Is China Policing My City? | Opinion*, Newsweek (Dec. 19, 2022, 6:00 AM), https://www.newsweek.com/why-china-policing-my-city-opinion-1767526#:~:text=Wanted%20since%20February%20in%20his%20home%20county%20of,Spanish%20judge%20would%20be%20unlikely%20to%20grant%20extradition..

[185] Press Release, Off. Pub. Affr's, *40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents*, U.S. Dep't Just. (May 12, 2022), https://www.justice.gov/opa/pr/united-states-signs-protocol-strengthen-international-law-enforcement-cooperation-combat.

[186] Valentin Weber, *The Dangers of a New Russian Proposal for a UN Convention on International Information Security*, Counc. on Foreign Rel.: Net Politics Blog (Mar. 21, 2023, 11:33 AM), https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security.

[187] Alexander Martin, *China proposes UN treaty criminalizes 'dissemination of false information'*, The Record (Jan. 16, 2023), https://therecord.media/china-proposes-un-treaty-criminalizing-dissemination-of-false-information.

[188] Lingling Wei et al., *China Locks Information on the Country Inside a Black Box*, Wall St. J. (Apr. 30, 2023, 6:13 PM), https://www.wsj.com/world/china/china-locks-information-on-the-country-inside-a-black-box-9c039928.

[189] Klon Kitchen & Bill Drexel, *When Foreign Adversaries Purchase Americans' Data*, Am. Enter. Instit. (Jun 1, 2021), https://www.aei.org/foreign-and-defense-policy/when-foreign-adversaries-purchase-americans-data/.

[190] Charles Dunst, *'How China Is Winning the Battle for Digital Sovereignty': A Review*, Counc. on Foreign Rel.: Asia Unbound Blog (Nov. 16, 2022, 2:22 PM), https://www.cfr.org/blog/how-china-winning-battle-digital-sovereignty-review.

[191] Jessica Dawson & Tarah Wheeler, How to tackle the data collection behind China's AI ambitions, Brookings (Apr. 29, 2022), https://www.brookings.edu/articles/how-to-tackle-the-data-collection-behind-chinas-ai-ambitions/.

[192] Frances G. Burwell & Kenneth Propp, Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy, Atlantic Council (Oct. 2022).

[193] Theodore Christakis (@TC_IntLaw), Twitter (Apr. 8, 2022, 4:00 AM) https://twitter.com/TC_IntLaw/status/1512339491092062216.

[194] *See* Vincent Voci et al., *Issue Briefing: The European Union's Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS): How "Sovereignty" Requirements Undermine Cybersecurity and Harm Transatlantic Ties*, U.S. Chamber of Commerce, (Dec. 5, 2022), https://www.uschamber.com/security/cybersecurity/issue-briefing-the-european-unions-proposed-cybersecurity-certification-scheme-for-cloud-services-eucs (recommending that the EUCS should not discriminate against entities merely over their geographic location).

the European Union[195] that the proposed sovereignty requirements are "of a political nature" and pointedly ask of the "immunity to non-EU law" standard: "[W]hat is the goal of this criteria?" Private[196]-sector[197] organizations[198] on both sides of the Atlantic[199] have also come out strongly against the contemplated requirements. (Whether the EUCS's draft immunity requirements are consistent[200] with EU legislation[201] and international trade commitments[202] is a separate and equally significant question.) It appears the various EU member states have made efforts[203] toward a compromise;[204] a joint document was circulated internally earlier this year that reportedly set out "six scenarios"[205] featuring immunity requirements at varying assurance levels.

Time may be running out. Earlier this month, the European Commission circulated ENISA's latest draft of the EUCS to a technical working group as a precursor to finalizing the scheme. This document,[206] which was leaked to the press,[207] continues to impose significant data localization and control requirements under the high assurance level. Also, "[a]dditional safeguards[208] have been introduced to put EU data outside the reach of third countries' jurisdiction," including mandatory EU choice-of-law and choice-of-forum contractual provisions. Notably, the draft high assurance level would also require the service provider "to

---

[195] Online Trust Coalition, Non-paper by DE, ES, FR and IT on the EUCS Requirements for Immunity to Non-EU Laws, (2021) (proposing revisions to the European Union Cloud Services Scheme, or "EUCS").
[196] Vincent Voci et al., *Issue Briefing: The European Union's Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS): How "Sovereignty" Requirements Undermine Cybersecurity and Harm Transatlantic Ties*, U.S. Chamber of Commerce, (Dec. 5, 2022), https://www.uschamber.com/security/cybersecurity/issue-briefing-the-european-unions-proposed-cybersecurity-certification-scheme-for-cloud-services-eucs.
[197] Cecilia Bonefeld-Dahl, Data Transfers in the Data Strategy: Understanding Myth and Reality, DigitalEurope (June 16, 2022).
[198] Comput. & Commc'n Indus. Ass'n, Joint Industry Statement on draft EU Cloud Certification Scheme, Comput. & Commc'n Indus. Ass'n (Dec. 1, 2022).
[199] CEE Digit. Coal., Central Eastern European Digital Industry's Appeal for Responsible Development of the European Cybersecurity Certification Scheme for Cloud Services (EUCS), CEE Digit. Coal. (Sept. 19, 2022).
[200] Matthias Bauer, Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements, European Centre for International Political Economy (March 2023).
[201] Bus. Software All., The Software Alliance's Comments to ANSSI on SecNumCloud (Version 3.2.A), Bus. Software All., (Nov. 2021).
[202] Info. Tech. Indus. Counc., Global Industry Concerns in European Cloud Security Certification, Info. Tech. Indus. Counc. (Dec. 8, 2021).
[203] Eu. Comm., Joint Document: Alternative Solutions Regarding the Issue of Independence to Non-EU Law in the context of EUCS, Eu. Comm. (last visited July 28, 2023); *see e.g.* Luca Bertuzzi, *EU countries seek way out of impasse on sovereignty requirements for cloud services*, Euractiv (Jan. 31, 2023), https://www.euractiv.com/section/cybersecurity/news/eu-countries-seek-way-out-of-impasse-on-sovereignty-requirements-for-cloud-services/ (referring to a document obtained from the European Commission exploring different approaches to digital sovereignty rules under the new EUCS).
[204] *Id*.
[205] *Id*.
[206] Eur. Union Agency for Cybersecurity, *Draft Version of EUCS – Cloud Services Scheme V1.0.319*, Eur. Union Agency for Cybersecurity (May 2023).
[207] Luca Bertuzzi, *Tech Brief: AI Act committee vote, EUCS tiered approach*, Euractiv (May 12, 2023), https://www.euractiv.com/section/all/news/tech-brief-ai-act-committee-vote-eucs-tiered-approach/.
[208] Lucca Bertuzzi, *EU Cloud Certification Headed for Tiered Approach on Sovereignty Criteria*, Euractiv (May 12, 2023), https://www.euractiv.com/section/cybersecurity/news/eu-cloud-certification-headed-for-tiered-approach-on-sovereignty-criteria/.

include[209] in [its] contract with the customer that it will only consider investigation requests issued under EU law or the national law of a member state"—an "immunity" formulation designed to engineer direct conflicts of law (or, more likely, to chase away global CSPs from seeking certification in the first place). Remarkably, the newly proposed "high+" standard goes even further by requiring providers "to put technical and organisational measures in place[210] to ensure that investigation requests from other jurisdictions are not considered." The draft scheme is a digital sovereigntist's dream.

Finding a solution that rejects the sovereignty-based approach is critical, because an EUCS that excludes U.S.-based CSPs[211] "would make the new Transatlantic Data Privacy Framework irrelevant, as U.S. firms would be precluded from managing a considerable amount of data in the EU, never mind transfer it overseas." The entire transatlantic project premised on the free flow of data for innovation and security could be at stake.

And cybersecurity standards are simply one front in a broader offensive. European data privacy regulators have consistently construed the "immunity to non-EU laws" principle as a proxy for GDPR compliance. In the immediate aftermath of *Schrems II*, for example, the French data protection authority, CNIL, famously recommended that entities handling French citizen health data[212] should avoid using U.S.-based CSPs. (A French judge ultimately, if reluctantly, disregarded this opinion,[213] not least because he believed[214] "European cloud providers weren't able to offer the same [quality] services" as U.S.-based ones.) Even since the negotiation of the DPF, with its seeming resolution of the key privacy law issues litigated in *Schrems II*, CNIL's sentiment holds: Last year, the agency endorsed the latest SecNumCloud revisions based expressly on the idea[215] that those revisions, including the Section 19.6 requirement that the relevant data "cannot be subject to non-European laws," were compliant "by design" with the GDPR. Earlier this year, the European Data Protection Board (EDPB) doubled down on this idea, publishing a report on public-sector use of cloud-based services[216] that stressed that

---

[209] *Id*.
[210] *Id*.
[211] Nigel Cory, *Europe's Cloud Security Regime Should Focus on Technology, Not Nationality*, Info. Tech. & Innovation Found. (Mar. 27, 2023), https://itif.org/publications/2023/03/27/europes-cloud-security-regime-should-focus-on-technology-not-nationality/.
[212] *See* Romain Dillet, *France's Health Data Hub to move to European cloud infrastructure to avoid EU-US data transfers*, TechCrunch (Oct. 12, 2020, 1:48 PM), https://techcrunch.com/2020/10/12/frances-health-data-hub-to-move-to-european-cloud-infrastructure-to-avoid-eu-us-data-transfers/ (reporting on the CNIL recommendation for French entities that "handle health data" ought to avoid using American cloud providers).
[213] Patrice Navarro & François Zannotti, *French Court refuses to suspend Microsoft's hosting of a public health data lake despite CNIL opinion (the Health Data Hub case - Part 2),* JDSupra (Oct. 22, 2020), https://www.jdsupra.com/legalnews/french-court-refuses-to-suspend-61424/.
[214] Catherine Strupp, *French Court Asks Microsoft for Safeguards Against U.S. Surveillance of Health Data*, Wall St. J. (Oct. 23, 2020, 5:30 AM), https://www.wsj.com/articles/french-court-asks-microsoft-for-safeguards-against-u-s-surveillance-of-health-data-11603445400.
[215] DataGuidance, *France: ANSSI Updates Certification Framework for Cloud Service Providers to Account for* Schrems II *Requirements, Endorsed by CNIL*, DataGuidance (Mar. 11, 2022), https://www.dataguidance.com/news/france-anssi-updates-certification-framework-cloud.
[216] Eur. Data Prot. Bd., 2022 Coordinated Enforcement Action Use of Cloud-Based Services by the Public Sector, Eur. Data Prot. Bd. (Jan. 17, 2023).

government agencies wishing to store information in the cloud should consider whether the hosting CSP is part of a multinational group that falls within the scope of "third country laws" that "also apply[ ] to data stored in the EEA"—a thinly veiled reference to the CLOUD Act. If so, avers the EDPB, then the mere possibility of the use of such a service could subject the agency to enforcement proceedings for violating the GDPR.

What's more, the "immunity to foreign law" principle could soon extend far beyond the realm of personal data covered by the GDPR. The European Commission's Data Act[217]—which also was proposed in early 2022 during the French presidency of the EU, and is likely to be approved and adopted in the coming weeks—covers non-personal data, "the most common type[218] of data to be shared across borders[.]" Designed to protect European industrial data from the purportedly prying eyes of foreign (read: American[219]) government officials, the Data Act's proposed Article 27[220] appears to "extend the consequences of *Schrems II*[221] to non-personal data" by requiring GDPR-style protection measures and adequacy analyses before such data can be transferred outside the EU. The imposition of these measures not only would reflect a hugely consequential weakening of the traditionally "rigid dualism[222]" in European privacy law doctrine between personal and non-personal data but also would mark a high point in the implementation of the sovereignty-based approach. Indeed, if novel immunity considerations[223] for cross-border transfers of non-personal data are combined with contemplated Data Act regulations that would "require cloud vendors[224] to obtain an EUCS certification"—which, as explained above, could impose such immunity considerations at the storage phase, before the transfer is even contemplated—then the triumph of the sovereignty-based vision over the entire lifecycle of European data would be complete.

* * *

[217] European Commission Press Release IP/22/1113, Data Act: Commission proposes measures for a fair and innovative data economy (Feb. 23, 2022).
[218] Kenneth Propp, *The EU's Proposed Data Act: Regulating International Flows of Non-Personal Data*, Cross-Border Data Forum (Dec. 10, 2021), https://www.crossborderdataforum.org/the-eus-proposed-data-act-regulating-international-flows-of-non-personal-data/.
[219] Commission Impact Assessment Report Accompanying the Document *Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)*, SWD (2022) 34 final (Feb. 23, 2022).
[220] Commission Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM (2022) 68 final (Feb. 23, 2022).
[221] Bárbara Da Rosa & Gianclaudio Malgieri, *The Data Act: a (slippery) third way beyond personal/non-personal data dualism?,* European Law Blog (May 4, 2023), https://europeanlawblog.eu/2023/05/04/the-data-act-a-slippery-third-way-beyond-personal-non-personal-data-dualism/.
[222] *Id*.
[223] Marco Leto Barone, *The EU Data Act and International Data Flows - Why Policymakers Should Clarify Art. 27 of the Data Act*, Info. Tech. Indus. Counc. (Mar. 2, 2023), https://www.itic.org/news-events/techwonk-blog/the-eu-data-act-and-international-data-flows-why-policymakers-should-clarify-art-27-of-the-data-act.
[224] Matthias Bauer, Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements, European Centre for International Political Economy (March 2023).

Respect for individual privacy binds Europe and the United States together. So, too, do extensive transatlantic commercial relationships and common security concerns. Certain European policymakers may feel as though the economic benefits of data flows move in one direction. But erecting "immunity" requirements—and justifying those requirements through flimsy security rationales—is not the answer. To the contrary, it is the free flow of data across borders, with appropriate consensus-based safeguards in place, that best preserves digital sovereignty and best promotes mutual trust and prosperity. Policymakers on both sides of the Atlantic have expended tremendous energy and resources in getting to the present moment. And much work remains to be done. They should capitalize on the current momentum and recognize the perils of alternative approaches.