Georgia's democratic development and falls short of any expectations of an EU candidate country."[45] A Venice Commission report concluded that new "measures are likely to have a chilling effect on the exercise of the freedoms of assembly and expression" and were "incompatible with the principles of lawfulness, necessity, and proportionality."[46]

Following the U.S. presidential election, Georgian Dream anticipated that it would have better relations with the United States under President Donald J. Trump. In the weeks leading up to President Trump's inauguration, Prime Minister Kobakhidze said that "[o]ur goal is to restart the relationship with the United States from scratch, to renew the strategic partnership, to do this with specific leadership."[47] Once President Trump was in office, Prime Minister Kobakhidze welcomed the suspension of U.S. foreign aid through USAID, which, he said, had been used by the United States "to cause unrest in various countries, to organize revolutions, to destabilize countries."[48] He added, in a reference to the foreign influence law, that "[w]e cannot allow attempts to destabilize our country to be financed from outside."[49] Prime Minister Kobakhidze aligned himself with the "peace efforts by President Trump," referring to the shift in the U.S. administration's support for Ukraine.[50] Thus far, the Trump administration has not reciprocated Prime Minister Kobakhidze's entreaties. The United States has not revoked the Biden administration's hold on U.S. assistance to the Georgian government or withdrawn the sanctions and visa restrictions that were imposed.

The Department of Justice Issues Regulations to Prevent Access to Americans' Bulk Sensitive Personal Data by Foreign Adversaries

doi:10.1017/ajil.2025.14

The U.S. Department of Justice has issued regulations to prevent access to Americans' bulk sensitive personal data by foreign adversaries.[1] The rules prohibit for the first time U.S.

[45] European Commission Press Release, Statement by High Representative/Vice-President Kaja Kallas and Commissioner for Enlargement Marta Kos on the Situation in Georgia (Feb. 7, 2025), *at* https://enlargement.ec.europa.eu/news/statement-high-representativevice-president-kaja-kallas-and-commissioner-enlargement-marta-kos-2025-02-07_en [https://perma.cc/V8SB-S62E].

[46] European Commission for Democracy Through Law (Venice Commission), Georgia – Urgent Opinion on Amendments to the Code of Administrative Offences and the Law on Assemblies and Demonstrations 14 (Mar. 3, 2025), *at* https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-PI(2025)004-e [https://perma.cc/JCT2-87QN].

[47] Премьер Грузии: для перезагрузки отношений с США «мы сделаем все» [*Georgian PM: We Will Do Everything to Reset Relations with the US*], SOVA (Dec. 30, 2024), *at* https://sovanews.tv/2024/12/30/premer-gruzii-dlya-perezagruzki-otnoshenij-s-ssha-my-sdelaem-vse.

[48] *Kobakhidze Welcomes Trump Administration's Suspension of Foreign Funding*, Civil Georgia (Jan. 31, 2025), *at* https://civil.ge/archives/658405.

[49] *Id.*

[50] *Kobakhidze Detracts Global Party of War and Deep State as Opposing "President Trump's Peace Efforts,"* Civil Georgia (Mar. 1, 2025), *at* https://civil.ge/archives/666572.

[1] *See* Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636 (Jan. 8, 2025) [hereinafter Final Rule]. The regulations

persons from entering into certain transactions that could give countries, like China, access to such data. The rules also restrict other transactions absent the implementation of specified security requirements.[2] The rules do not cover U.S. government collection of commercially available information, nor is their purpose to protect privacy interests.[3] Concerns about foreign access to U.S. personal data, through illicit acts (like hacking) and lawful measures (such as collecting and purchasing publicly available information), have existed for years.[4] Yet, U.S. law and policy have generally opposed the imposition of limits on private sector cross-border data flows. Committee on Foreign Investment in the United States (CFIUS) review and rejection of transactions, like that for TikTok, due to data security concerns have been the exception and are of limited scope.[5] The new regulations, together with other recent rules and governmental actions, signal a change in approach.[6] The shift reflects a fear in U.S. law

implement an executive order. *See* Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, Exec. Order 14117, 89 Fed. Reg. 15421 (Feb. 28, 2024) [hereinafter Executive Order].

[2] *See* Cybersecurity and Infrastructure Security Agency, Security Requirements for Restricted Transactions (Jan. 2025), *at* https://www.cisa.gov/sites/default/files/2025-01/Security_Requirements_for_Restricted_Transaction-EO_14117_Implementation508.pdf [https://perma.cc/BD4V-CUTB].

[3] On the U.S. government's collection of the personal data of Americans, see, for example, Byron Tau, Andrew Mollica, Patience Haggin & Dustin Volz, *How Ads on Your Phone Can Aid Government Surveillance*, WALL ST. J. (Oct. 13, 2023), *at* https://www.wsj.com/tech/cybersecurity/how-ads-on-your-phone-can-aid-government-surveillance-943bde04; Byron Tau & Dustin Volz, *U.S. Spy Agencies Buy Vast Quantities of Americans' Personal Data, U.S. Says*, WALL ST. J. (June 12, 2023), *at* https://www.wsj.com/articles/u-s-spy-agencies-buy-vast-quantities-of-americans-personal-data-report-says-f47ec3ad; and Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020), *at* https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600. *See generally* Office of the Director of National Intelligence Senior Advisory Group Panel on Commercially Available Information, Report to the Director of National Intelligence (Jan. 27, 2022), *at* https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [https://perma.cc/26S8-4EBW].

[4] *See, e.g.*, Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community 26 (Feb. 6, 2023), *at* https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf [https://perma.cc/TD3B-QF9E]; National Counterintelligence & Security Center, China's Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security (Feb. 2021), *at* https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf [https://perma.cc/8ETC-4J7Z].

[5] CFIUS's concern with the data security consequences of Chinese investments in U.S. businesses is longstanding, resulting for example in the aborted merger of MoneyGram and Ant Financial in 2018. *See* Ana Swanson & Paul Mozur, *MoneyGram and Ant Financial Call Off Merger, Citing Regulatory Concerns*, N.Y. TIMES (Jan. 2, 2018), *at* https://www.nytimes.com/2018/01/02/business/moneygram-ant-financial-china-cfius.html. Congress expanded CFIUS jurisdiction over investments involving sensitive personal data in the Foreign Investment Risk Review Modernization Act. *See* 50 U.S.C. § 4565(a)(4)(B)(iii)(III). President Biden's executive order on CFIUS specifically directed the review of transactions pertaining to sensitive data. *See* Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States, Exec. Order 14083, Sec. 3(c), 87 Fed. Reg. 57369 (Sept. 15, 2022). CFIUS, most famously, recommended that Chinese-owned ByteDance be required to divest its interest in TikTok. President Donald J. Trump endorsed that recommendation, resulting in litigation and settlement negotiations that continued during the Biden administration. In 2024, Congress enacted a law that would require divestment. *See* Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. 118-50, Div. H, 138 Stat. 895, 955 (Apr. 24, 2024). The Supreme Court found the statute constitutional. *See* TikTok v. Garland, Nos. 24-656 & 24-257 (Jan. 17, 2025). President Trump, however, upon re-entering office, ordered the attorney general not to enforce the law for seventy-five days. *See* Application of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok, Exec. Order 14166, 90 Fed. Reg. 8611 (Jan. 20, 2025).

[6] *See, e.g.*, Protecting Americans' Sensitive Data from Foreign Adversaries, Exec. Order 14034, 86 Fed. Reg. 31423 (June 9, 2021); Securing the Information and Communications Technology and Services Supply Chain;

https://doi.org/10.1017/ajil.2025.14 Published online by Cambridge University Press

enforcement and national security agencies that existing rules are insufficient to counter the increasing risk of electronic espionage by China and other countries stemming from the proliferation of data, data collection, data sales, and the development of artificial intelligence technologies and other forms of data analysis.[7]

Data flows are a staple of international commerce and communications; they can transmit ideas and norms; they can promote human rights and global health; and they can be misused by private and public actors to impose privacy harms and create national security risks. Despite the harms and risks, U.S. policy, across administrations, has championed the free cross-border flow of information and has sought to establish international norms and mechanisms that limit the regulation of transnational data transfers. The United States initiated and promoted the Declaration on the Future of the Internet, which committed signatories to "[p]romote [their] work to realize the benefits of data free flows."[8] In the context of the G7, it has supported the Data Free Flow with Trust concept first proposed by Japan.[9] It has backed the Global Cross-Border Privacy Rules Forum, which included as one of its objectives support for the free flow of data.[10] In trade agreements and fora, the United States has proposed policies that safeguard cross-border data flows, prohibited data localization requirements, and restricted government access to software source code.[11]

But U.S. support for unrestricted data flows abruptly shifted in late 2023. At a meeting of the World Trade Organization's Joint Statement Initiative on Electronic Commerce, the United States withdrew a proposal, first made in 2019 during the Trump administration,[12] that took a strong position in favor of free cross-border data flows and against data localization and software source code review.[13] Announcing the decision, the Office of the U.S. Trade Representative (USTR) stated that "[m]any countries, including the United States, are examining their approaches to data and source code, and the impact of trade rules in these areas. In order to provide enough policy space for those debates to unfold, the United States has removed its support for proposals that might prejudice or hinder those

Connected Software Applications, 88 Fed. Reg. 39353 (June 16, 2023); Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360 (Jan. 16, 2025); Protecting Americans' Data from Foreign Adversaries Act, Pub. L. 118-50, Div. I, 138 Stat. 895, 960 (Apr. 24, 2024).

[7] *See, e.g.*, National Counterintelligence & Security Center, National Counterintelligence Strategy 2024, at 13 (Aug. 1, 2024), *at* https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf [https://perma.cc/73GJ-FEFR].

[8] A Declaration for the Future of the Internet (Apr. 2022), *at* https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf [https://perma.cc/F5PP-86XQ].

[9] *See* G7 Hiroshima Leaders' Communiqué, 28–29 (May 20, 2023), *at* https://www.mofa.go.jp/policy/economy/summit/hiroshima23/documents/pdf/Leaders_Communique_01_en.pdf [https://perma.cc/G9J8-G6M8].

[10] *See* U.S. Dept. of Commerce, Global Cross-Border Privacy Rules Declaration (Apr. 2022), *at* https://www.commerce.gov/global-cross-border-privacy-rules-declaration [https://perma.cc/3TPG-SAKN].

[11] *See* Agreement Between the United States of America and Japan Concerning Digital Trade, Arts. 11–12, TIAS 20-101.1 (Oct. 7, 2019); Agreement Between the United States of America, the United Mexican States, and Canada, Arts. 19.11–19.12 (Nov. 30, 2018).

[12] *See* Communication from the United States, WTO Doc. INF/ECOM/6 (Mar. 25, 2019).

[13] *See* David Lawder, *US Drops Digital Trade Demands at WTO to Allow Room for Stronger Tech Regulation*, Reuters (Oct. 25, 2023), *at* https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25.

https://doi.org/10.1017/ajil.2025.14 Published online by Cambridge University Press

domestic policy consideration."[14] Soon thereafter, USTR also paused Indo-Pacific Economic Framework for Prosperity talks on digital trade.[15] USTR's decisions drew protests from the business community, which benefits from open data borders and international restrictions on the domestic regulation of data transfers, and a mixed reception in Congress, where some have argued for a trade policy that reserves leeway for greater domestic digital governance.[16]

USTR did not provide a full explanation for the announced policy shift, but U.S Trade Representative Katherine Tai offered some insight into the decision in remarks she gave early in 2024.[17] Ambassador Tai noted the transformation in the role of data in international transactions over the past two decades from facilitating traditional transactions (in goods) to becoming the subject of the transaction itself. This change, she explained, "give[s] you a sense . . . that there are much, much bigger equities at stake than what we might be doing in our trade negotiations."[18] Before making additional international commitments, she said, the United States needed to give further consideration to "how we regulate data, . . . how we regulate the companies that accumulate, harvest, and trade in this data," and the relationship between "trade [in data] and national security."[19]

Ambassador Tai's comments on data and national security foreshadowed President Biden's issuance, just a couple of weeks later, of an executive order on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."[20] The order directed the attorney general to issue regulations restricting the sale of personal information by data brokers to adversaries "when such access would pose an unacceptable risk to the national security of the United States."[21] Uncontrolled access to Americans' personal data constituted, according to the order, an "unusual and

[14] USTR Press Release, USTR Statement on WTO E-Commerce Negotiations (Oct. 24, 2023), *at* https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations [https://perma.cc/K2KU-NXAY].

[15] *See* David Lawder, *U.S. Suspends Indo-Pacific Talks on Key Aspects of Digital Trade – Lawmakers*, REUTERS (Nov. 8, 2023), *at* https://www.reuters.com/business/finance/us-suspends-indo-pacific-talks-key-aspects-digital-trade-lawmakers-2023-11-08.

[16] *See, e.g.*, Letter from Elizabeth Warren and Eleven Other Members of Congress to President Joseph R. Biden, Jr. (Nov. 6, 2023), *at* https://www.warren.senate.gov/imo/media/doc/FINAL%20Letter%20to%20Biden%20in%20Support%20of%20USTR%20Digital%20Trade%20Work.pdf [https://perma.cc/AP2X-GEBL]; U.S. Senate Committee on Finance Press Release, Wyden Statement on Ambassador Tai's Decision to Abandon Digital Trade Leadership to China at WTO (Oct. 25, 2023), *at* https://www.finance.senate.gov/chairmans-news/wyden-statement-on-ambassador-tais-decision-to-abandon-digital-trade-leadership-to-china-at-wto [https://perma.cc/6BS4-EEXA]; Senator Mike Crapo Press Release, Crapo and Colleagues Condemn Biden Administration's Decision to Cede U.S. Digital Leadership to China (Oct. 26, 2023), *at* https://www.crapo.senate.gov/media/newsreleases/crapo-and-colleagues-condemn-biden-administrations-decision-to-cede-us-digital-leadership-to-china [https://perma.cc/35N8-2NKP]; U.S. Chamber of Commerce Press Release, U.S. Chamber and Other Associations Letter to NSC/NEC on Digital Trade (Nov. 7, 2023), *at* https://www.uschamber.com/international/trade-agreements/u-s-chamber-and-other-associations-letter-to-nsc-nec-on-digital-trade [https://perma.cc/KY4X-HAC4].

[17] *See* Council on Foreign Relations, C. Peter McColough Series on International Economics with Katherine Tai (Feb. 12, 2024), *at* https://www.cfr.org/event/c-peter-mccolough-series-international-economics-katherine-tai-0 [https://perma.cc/NT64-9MQS].

[18] *Id.*

[19] *Id.*

[20] *See* Executive Order, *supra* note 1. The order was founded on the president's constitutional authority and that provided by the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701, et seq.

[21] Executive Order, *supra* note 1, Sec. 1.

https://doi.org/10.1017/ajil.2025.14 Published online by Cambridge University Press

extraordinary threat."[22] Adversaries could "use access to bulk data sets to fuel the creation and refinement of AI and other advanced technologies, thereby improving their ability to exploit the underlying data."[23] They could use "sensitive personal data linked to populations and locations associated with the Federal Government—including the military— . . . to reveal insights . . . that threaten national security."[24] They could use data "to track and build profiles on United States individuals, including Federal employees and contractors, for illicit purposes, including blackmail and espionage."[25] And they could use data "to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb dissent or political opposition; otherwise limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties."[26] "Buying data through data brokers is currently legal in the United States," a senior administration official commented, "and that reflects a gap in our national security tool kit that we're working to fill."[27]

The new Department of Justice regulations implementing the order limit commercial transactions involving bulk U.S. sensitive personal data or government-related data.[28] U.S. persons are prohibited from engaging in data brokerage transactions with a "country of concern" or a "covered person" that involves any access to such data.[29] "Countries of concern" include China, Cuba, Iran, North Korea, Russia, and Venezuela.[30] A "covered person" is a non-U.S. individual who is primarily a resident of a country of concern, is an employee or contractor of a covered entity, or is a person designated as such by the attorney general.[31] A "covered person" is also a non-U.S. entity that is organized or has its principal place of business in a country of concern or is more than 50 percent owned by a country of concern or covered persons.[32] Other transactions—those involving vendor agreements, employment agreements, and investment agreements—are restricted, that is they are prohibited unless the U.S. person complies with U.S. Cybersecurity and

[22] *Id.*, pmbl.
[23] *Id.*
[24] *Id.*
[25] *Id.*, Sec. 1.
[26] *Id.*
[27] Dustin Volz & Lingling Wei, *U.S. Limits Sales of Americans' Personal Data to China, Other Adversaries*, WALL ST. J. (Feb. 28, 2024), *at* https://www.wsj.com/politics/national-security/u-s-to-limit-sales-of-americans-personal-data-to-china-other-adversaries-e82a3ca5.
[28] Final Rule, *supra* note 1, at 1639. "Government-related data" includes as certain geolocation data for any location within any area that's identified in a list included in the regulation. *See id.* at 1712 (adding 28 C.F.R. § 202.222(a)). It also includes sensitive personal data that is linked or linkable to current or recent former U.S. government employees or contractors, or former senior officials. *See id.* "U.S. sensitive personal data" is defined as "covered personal identifiers, precise geolocation data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof." *See id.* at 1716 (adding 28 C.F.R. § 202.249).The definition of the adjective "bulk" is based on exceeding a certain threshold, which varies by data category. *See id.* at 1708 (adding 28 C.F.R. § 202.205).
[29] *See id.* at 1717 (adding 28 C.F.R. § 202.301). It also prohibited human 'omic data transactions, transactions with non-covered persons that lack restrictions on subsequent transactions, and evading or directing prohibited transactions. *See id.* at 1718–19 (adding 28 C.F.R. §§ 202.303–202.305).
[30] *See id* at 1725 (adding 28 CFR § 202.601(a)).
[31] *See id.* at 1708–09 (adding 28 C.F.R. § 202.211); *see also id.* at 1725 (adding 28 C.F.R. § 202.701).
[32] *See id.*

https://doi.org/10.1017/ajil.2025.14 Published online by Cambridge University Press

Infrastructure Security Agency-issued security requirements and has developed and implemented a data compliance program and conducted an audit.[33] Certain types of transactions that might otherwise have been prohibited or restricted are exempted (such as those pertaining to scientific research), and applications for licenses can be made.[34] Civil and criminal penalties apply to violations.[35]

Sensitive to the significance of these new prohibitions and restrictions on data transactions, the executive order reiterated the United States' continued commitment to "supporting a vibrant, global economy by promoting cross-border data flows required to enable international commerce and trade; and facilitating open investment."[36] The order made clear that it did "not authorize the imposition of generalized data localization requirements."[37] It also clarified that it did "not broadly prohibit United States persons from conducting commercial transactions . . . with entities and individuals" from countries of concern or "impose measures aimed at a broader decoupling of the substantial consumer, economic, scientific, and trade relationships that the United States has with other countries."[38]

Though the new rule is consistent with the new Trump administration's stance on China, its future is unclear.[39]

International Criminal Law

Secretary of State Blinken Concludes that the Rapid Support Forces Have Committed Genocide in Sudan

doi:10.1017/ajil.2025.13

In early January 2025, U.S. Secretary of State Antony J. Blinken announced his conclusion that the Rapid Support Forces (RSF) and its associated militias had committed genocide in Sudan during the civil war that has decimated that country for the past two years.[1] At the same

[33] *See id.* at 1719, 1728 (adding 28 C.F.R. §§ 202.401, 202.1001, 202.1002).

[34] *See id.* at 1721 (adding 28 C.F.R. §§ 202.506, 220.507).

[35] *See id.* at 1730 (adding 28 C.F.R. § 202.1301). The penalties are those that apply under Section 206 of IEEPA, 50 U.S.C. § 1705.

[36] Executive Order, *supra* note 1, Sec. 1.

[37] *Id.*

[38] *Id.*

[39] President Trump's regulatory freeze memorandum directed all federal departments and agencies to consider postponing rules, like the bulk sensitive data regulations, that were published in the *Federal Register* but not yet in effect. *See* Regulatory Freeze Pending Review, para. 3, 90 Fed. Reg. 8249 (Jan. 20, 2025). The Executive Order, *supra* note 1, that serves as the legal basis for the regulations was not among the orders rescinded by President Trump upon assuming office. *See* Initial Rescissions of Harmful Executive Orders and Actions, Exec. Order 14148, 90 Fed. Reg. 8237 (Jan. 20, 2025).

[1] *See* U.S. Dep't of State Press Release, Genocide Determination in Sudan and Imposing Accountability Measures (Jan. 7, 2025), *at* https://2021-2025.state.gov/genocide-determination-in-sudan-and-imposing-accountability-measures [https://perma.cc/6KU9-ULQ3] [hereinafter Genocide Determination]. An RSF spokesperson rejected the charges. *See* Daphne Psaledakis, David Lewis & Nafisa Eltahir, *US Determines Sudan's RSF Committed Genocide, Imposes Sanctions on Leader*, Reuters (Jan. 8, 2025), *at* https://www.reuters.com/world/us-impose-sanctions-sudan-rsf-leader-dagalo-sources-say-2025-01-07. This is the eighth time that the U.S. government has declared a genocide subsequent to the Cold War. *See* Katharine Houreld, *U.S. Declares Genocide in*