# CONTEMPORARY PRACTICE OF THE UNITED STATES RELATING TO INTERNATIONAL LAW

EDITED BY JEAN GALBRAITH*

***In this section:***



* Maura Douglas, Patricia Liverpool, David Peters, Sabrina Ruchelli, Jenna Smith, Kristen Dewilde, and Brian Yeh contributed to the preparation of this section.



https://doi.org/10.1017/ajil.2018.61 Published online by Cambridge University Press

## General International and U.S. Foreign Relations Law

### *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*

doi:10.1017/ajil.2018.61

On March 22, 2018, Congress passed a $1.3 trillion omnibus spending bill that President Trump signed into law the following day, thus narrowly avoiding a government shutdown.[1] Included within the voluminous bill is the Clarifying Lawful Overseas Use of Data (CLOUD) Act,[2] which enhances both the United States' and foreign nations' access to cross-border electronic data for law enforcement purposes.[3]

Prompted by the challenge of collecting "electronic evidence necessary to enforce essential laws in an increasingly international and digital age," the CLOUD Act makes two distinct yet related changes to the law governing cross-border access to data in criminal investigations.[4] First, the Act amends the Stored Communications Act (SCA)—a "dense and confusing" statutory scheme that protects "the privacy of stored Internet communications"[5]—by "explicitly requiring providers subject to the jurisdiction of the United States to produce data pursuant to appropriate SCA process, even if the provider chooses to store that data outside the United States."[6] The SCA had been passed in 1986 as part of a larger bill, the Electronic Communications Privacy Act (ECPA).[7] As a second change, the CLOUD Act amends several other provisions of the ECPA to create a framework that allows U.S. service providers to disclose U.S.-stored data to certain foreign countries pursuant to lawful foreign orders.[8] According to Acting Deputy Assistant Attorney General Richard Downing, the provisions together "build a new framework for effective, efficient cross-border access to data that protects both legitimate privacy interests and our public safety and national security, and benefits U.S. business interests as well."[9]

[1] Consolidated Appropriations Act of 2018, Pub. L. No. 115-141, 132 Stat. 348 (2018) [hereinafter 2018 Appropriations Act]; *see also* Julie Hirschfield Davis & Michael D. Shear, *Trump Signs Spending Bill, Reversing Veto Threat and Avoiding Government Shutdown*, N.Y. Times (Mar. 23, 2018), *at* https://www.nytimes.com/2018/03/23/us/politics/trump-veto-spending-bill.html.

[2] 2018 Appropriations Act, *supra* note 1, div. 5; *see also* Robyn Greene, *Somewhat Improved, the CLOUD Act Still Poses a Threat to Privacy and Human Rights*, Just Security (Mar. 23, 2018), *at* https://www.justsecurity.org/54242/improved-cloud-act-poses-threat-privacy-human-rights (observing that, as a "quintessential must-pass bill," the "2,232 page omnibus bill to fund the government" was used "as a vehicle to quietly pass through the controversial CLOUD Act").

[3] *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 15 (2017) (statement of Richard W. Downing, Acting Deputy Assistant Attorney General, Dep't of Justice) [hereinafter Downing Testimony].

[4] *Id.* at 7.

[5] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1208 (2004).

[6] Downing Testimony, *supra* note 3, at 11.

[7] Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848, 1860 (1986); *see also* Kerr, *supra* note 5, at 1208 n.2 (noting the various names used for the SCA over time).

[8] Downing Testimony, *supra* note 3, at 13.

[9] *Id.* at 2.

The Obama administration first introduced draft legislation for what would become the CLOUD Act on July 15, 2016.[10] Originally, the proposed legislation did not include language addressing how the SCA applied to data stored abroad by U.S. communications service providers. But the day before the draft legislation was to be released, the Second Circuit held in *Microsoft Corp. v. United States* that the SCA did not authorize the issuance of a warrant to obtain data held by a U.S. provider where this data was stored abroad—in this case, in Ireland.[11] Even though the Department of Justice petitioned for and obtained Supreme Court review of the decision,[12] the *Microsoft* holding prompted the Obama and then the Trump administrations to seek a legislative fix. As Assistant Attorney General Peter Kadzik explained in a cover letter accompanying the initial draft legislation:

> Yesterday, the United States Court of Appeals for the Second Circuit held in *Microsoft Corp. v. United States* that section 2703 of ECPA does not authorize our courts to issue and enforce warrants served on U.S. providers to obtain electronic communications stored abroad. If the decision stands[,] . . . [t]he Administration intends to promptly submit legislation to Congress to address the significant public safety implications of the *Microsoft* decision. This will be a necessary addition to the proposal that we are submitting today.[13]

The CLOUD Act—enacted a mere three weeks after the Supreme Court heard oral arguments in *Microsoft Corp.*, but before a decision was handed down[14]—resolved the issue of the SCA's application to data stored abroad by U.S. providers and thus mooted the pending controversy.[15] Congress added a provision to the SCA clarifying that:

[10] Letter from Peter J. Kadzik, Assistant Attorney General, Dep't of Justice, to Hon. Joseph R. Biden, President, U.S. Senate 3–4 (July 15, 2016), *available at* https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p1 [https://perma.cc/7WGW-5D6G] [hereinafter Kadzik Letter]; *see also* David Kris, *U.S. Government Presents Draft Legislation for Cross-Border Data Requests*, LAWFARE (July 16, 2016), *at* https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests.

[11] 829 F.3d 197 (2d Cir. 2016).

[12] United States v. Microsoft Corp., 138 S. Ct. 356 (2017) (*cert. granted*).

[13] Kadzik Letter, *supra* note 10, at 2–3; *see also* Downing Testimony, *supra* note 3, at 2 (including within the proposal to Congress "legislation to fix the problems created by the *Microsoft* decision").

[14] *See* Nina Totenberg, *A Needle in a Legal Haystack Could Sink a Major Supreme Court Privacy Case*, NPR (Mar. 28, 2018), *at* https://www.npr.org/2018/03/28/597444394/a-needle-in-a-legal-haystack-could-sink-a-major-supreme-court-privacy-case (noting that "a Congress famous for gridlock passed legislation to modernize" the SCA "just three weeks after the Supreme Court argument").

[15] Following the passage of the CLOUD Act, the U.S. Department of Justice obtained a new warrant for the Microsoft data stored abroad. *See* Motion to Vacate the Judgment of the Court of Appeals and Remand the Case with Directions to Dismiss as Moot, 2, United States v. Microsoft Corp., No. 17-2 (Mar. 30, 2018). The Solicitor General then petitioned the Court to vacate the judgment of the court of appeals and remand the case with directions to dismiss as moot because "Microsoft's sole objection—that the prior warrant was impermissibly extraterritorial—no longer applies." *Id.* at 1–2. Microsoft did not oppose the government's request, "provided that the Court similarly vacates the opinion of the magistrate judge (as adopted by the District Court) that the Second Circuit reversed. . . ." Response to the United States' Motion to Vacate and Remand with Directions to Dismiss as Moot, 2, United States v. Microsoft Corp., No. 17-2 (Apr. 3, 2018).

On April 17, the Court issued a *per curiam* opinion agreeing "[n]o live dispute remains between the parties" and "[t]his case, therefore, has become moot." United States v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018) (per curiam). As such, the Court ruled "the judgment on review is accordingly vacated, and the case is remanded" to the court of appeals "with instructions first to vacate the District Court's contempt finding and its denial of Microsoft's motion to quash, then to direct the District Court to dismiss the case as moot." *Id.*

https://doi.org/10.1017/ajil.2018.61 Published online by Cambridge University Press

> A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, *regardless of whether such communication, record, or other information is located within or outside of the United States*.[16]

Congress also created a limited mechanism for providers to challenge these warrants where applying the SCA to data stored overseas might create "conflicting legal obligations" by requiring "disclosure of electronic data that foreign law prohibits communications-service providers from disclosing."[17] At present, this mechanism is a nascent one. It applies only where "qualifying foreign governments" are concerned, with such governments defined as ones with whom the United States has reached executive agreements on access to data.[18] As discussed below, no such agreements presently exist.[19] If such agreements are reached in the future, then, following a motion by the communications service provider, a reviewing court may modify or quash a warrant

> only if the court finds that—(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government; (ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and (iii) the customer or subscriber is not a United States person and does not reside in the United States.[20]

In determining whether "the interests of justice dictate that the legal process should be modified or quashed," Congress requires a reviewing court to conduct a "comity analysis."[21] The reviewing court "shall take into account, as appropriate," eight enumerated factors, including "the interests of the United States," "the interests of the qualifying foreign government in preventing any prohibited disclosure," and the "likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider."[22]

In addition to this limited mechanism, the CLOUD Act specifies that it does not "modify or otherwise affect the common law standards governing the availability or application of comity analysis."[23] It remains to be seen whether challenges to particular warrants based

[16] 2018 Appropriations Act, *supra* note 1, div. 5, § 103(a)(1) (to be codified at 18 U.S.C. § 2713) (emphasis added). Downing's testimony indicates that the Department of Justice views this language as applicable to "providers subject to the jurisdiction of the United States." *See* Downing Testimony, *supra* note 3, at 11.

[17] 2018 Appropriations Act, *supra* note 1, at div. 5, § 102(5). Downing testified that as of 2016 "[the Department of Justice] is not aware of any instance in which a provider has informed the Department or a court that production pursuant to the SCA of data stored outside the United States would place the provider in conflict with local law." Downing Testimony, *supra* note 3, at 11.

[18] 2018 Appropriations Act, *supra* note 1, at div. 5, § 103(b) (to be codified at 18 U.S.C. § 2703(h)).

[19] *See infra* notes 29–48 and accompanying text.

[20] 2018 Appropriations Act, *supra* note 1, at div. 5, § 103(b) (to be codified at 18 U.S.C. § 2703(h)).

[21] *Id.*

[22] *Id.* The mechanism to challenge extraterritorial warrants was a late addition to the CLOUD Act—the draft legislation introduced by both the Obama and Trump administrations did not include the provisions establishing it. *See* Kadzik Letter, *supra* note 10, at 4 (failing to include such provisions in draft legislation); *see also* Downing Testimony, *supra* note 3, at 24 (same).

[23] 2018 Appropriations Act, *supra* note 1, at div. 5, § 103(c).

https://doi.org/10.1017/ajil.2018.61 Published online by Cambridge University Press

on common-law comity principles will be made going forward, particularly in the wake of the recent implementation of the European Union's General Data Protection Regulation.[24]

Besides clarifying the scope of U.S. law enforcement's authority to access data stored abroad, the CLOUD Act also creates a framework to facilitate access by certain foreign governments to data stored by U.S. service providers in the United States. Kadzik explained the need for such a framework when introducing the draft legislation:

> Foreign governments investigating criminal activities abroad increasingly require access to electronic evidence from U.S. companies that provide electronic communications services to millions of their citizens and residents. Such data is often stored or accessible only in the United States, where U.S. law, including the ECPA, limits the companies' ability to disclose it.[25]

According to Kadzik and others,[26] the current method for processing requests by foreign governments for U.S.-stored data—the use of Mutual Legal Assistance Treaties (MLATs)—is too labor intensive and time consuming to handle the "significant increases in the volume and complexity of requests . . . in the Internet Age."[27]

The CLOUD Act thus allows U.S. providers to disclose data to a limited set of foreign governments who are targeting the accounts of non-U.S. persons located outside the United States.[28] A foreign government is eligible for such disclosures under the CLOUD Act only after entering into an "executive agreement" with the U.S. government.[29] Moreover, the attorney general must, with the concurrence of the secretary of state, submit a written certification to Congress that the "executive agreement" satisfies four statutory requirements set forth in the newly enacted 18 U.S.C. § 2523.[30]

[24] *See* Jennifer Daskal, Microsoft Ireland, *the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9, 11–13 (2018) (noting potential tensions between this EU regulation and warrants that may be issued pursuant to the CLOUD Act).

[25] Kadzik Letter, *supra* note 10, at 1.

[26] Downing testified that the MLAT process is "not devised to handle the growing demands for digital evidence. Already, the Department faces significant challenges in responding to the enormous volume of foreign demands with the requisite speed." Downing Testimony, *supra* note 3, at 7. For further discussion on how MLATs operate and the need for reform, see generally Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687 (2016); Peter Swire, Justin Hemmings & Suzanne Vergnolle, *A Mutual Legal Assistance Case Study: The United States and France*, 34 WIS. INT'L L.J. 323 (2017).

[27] Kadzik Letter, *supra* note 10, at 1; *see also* Swire & Hemmings, *supra* note 26, at 700 (noting that on average the MLAT process takes approximately ten months to execute valid electronic evidence requests).

[28] *See* Downing Testimony, *supra* note 3, at 13. The CLOUD Act does not require disclosure as a matter of U.S. law, but where applicable it means that U.S. law will no longer operate as a bar to disclosure. *See id.*

[29] 2018 Appropriations Act, *supra* note 1, at div. 5, § 104 (to be codified in various sections of 28 U.S.C.); *see also* STEPHEN P. MULLIGAN, CONGRESSIONAL RESEARCH SERVICE REPORT ON CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT 15–16 (Apr. 23, 2018), *available at* https://fas.org/sgp/crs/misc/R45173.pdf (concluding that the CLOUD Act "authorizes" such executive agreements and thus serves as a "source of authority" for the executive branch to enter into them). MLATs remain the vehicle for processing cross-border data requests for those nations that do not enter into the bilateral data-sharing agreements described in the CLOUD Act. *See* Downing Testimony, *supra* note 3, at 9.

[30] 2018 Appropriations Act, *supra* note 1, at div. 5, § 105 (to be codified at 18 U.S.C. § 2523). While the attorney general's determination "shall not be subject to judicial or administrative review," the CLOUD Act creates expedited legislative procedures that Congress could use in passing a joint resolution of disapproval blocking the agreement within 180 days of the certification's submission to Congress. *See id.*

https://doi.org/10.1017/ajil.2018.61 Published online by Cambridge University Press

First, the attorney general must certify that "the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement."[31] Further, the statute enumerates specific "factors to be met in making such a determination," including whether the foreign government "demonstrates respect for the rule of law and principles of nondiscrimination" and "adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights," among others.[32]

Second, the attorney general must also certify that "the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement."[33] Third, "the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data."[34]

Fourth, and finally, the attorney general must certify that the executive agreement requires "any order that is subject to the agreement" to comply with several enumerated restrictions.[35] Among other requirements, the agreement must provide that "the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement."[36] Further, an order issued pursuant to the agreement "shall be for the purpose of obtaining information relating to . . . serious crime" and "shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order."[37] And, the "United States Government shall reserve the right to render the agreement inapplicable as to any order for which the United States Government concludes the agreement may not properly be invoked."[38]

According to the executive branch, the CLOUD Act "meet[s] the legitimate public safety needs of other countries," while "establish[ing] adequate baselines for protecting privacy and civil liberties."[39] But the changes the CLOUD Act makes to the law of cross-border access to data has engendered substantial disagreement among scholars, industry, and civil liberty organizations as to whether the Act "is good for privacy and human rights."[40] On the one hand, organizations including the Electronic Frontier Foundation and ACLU campaigned against the CLOUD Act on the grounds that the bill "fails to protect the rights of Americans and

[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Downing Testimony, *supra* note 3, at 13–14.
[40] Jennifer Daskal & Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, LAWFARE (Mar. 14, 2018), *at* https://lawfareblog.com/why-cloud-act-good-privacy-and-human-rights. Criticism was also levied at the process of the CLOUD Act's enactment: "It was never . . . marked up by any committee in either the House or the Senate. . . . It was robbed of a stand-alone floor vote because Congressional leadership decided, behind closed doors, to attach this unvetted, unrelated data bill to the $1.3 trillion government spending bill." David Ruiz, *Responsibility Deflected, the CLOUD Act Passes*, ELECTRONIC FRONTIER FOUND. (Mar. 22, 2018), *at* https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes.

https://doi.org/10.1017/ajil.2018.61 Published online by Cambridge University Press

individuals abroad, and would place too much authority in the hands of the executive branch with few mechanisms to prevent abuse."[41] On the other hand, leading U.S. tech companies voiced public support for the CLOUD Act's passage, arguing that it "reflects a growing consensus in favor of protecting Internet users around the world and provides a logical solution for governing cross-border access to data."[42] And privacy scholars Jennifer Daskal and Peter Swire argue that the CLOUD Act improves "privacy and civil liberties protections compared to a world without such legislation" by "set[ting] critically important baseline substantive and procedural protections, while doing so in a way that is achievable and understandable to other rights-respecting nations."[43]

The effect on digital privacy may be felt sooner rather than later, as the CLOUD Act's enactment paves the way for the finalization of a bilateral data-sharing agreement between the United States and the United Kingdom. Prompted by the need to address the "untenable situation in which . . . Britain cannot quickly obtain data for domestic probes because it happens to be held by companies in the United States," undisclosed negotiations between the two allies were underway at least by February of 2016.[44] American and British officials alike held up the potential U.S.–U.K. agreement as both a reason for passing the bill and a model for future bilateral executive agreements. As Downing testified during congressional hearings on the CLOUD Act:

> Under this approach, the United States and a foreign government can negotiate a bilateral agreement setting forth the terms for cross-border access to data, but only with those countries who share the United States' commitment to the rule of law and respect for privacy and civil liberties. . . . The United States has for some time been working on a proposed agreement of this sort with the United Kingdom, which has made clear that its inability to access data from U.S. providers in an efficient and effective way poses a very serious threat to public safety and national security in the United Kingdom. . . . If the approach proves successful, we would consider it for other appropriate countries as well.[45]

The CLOUD Act's sponsor, Senator Orrin Hatch, called the U.S.–U.K. agreement "a model for future agreements between the United States and other countries" and advocated for

[41] CLOUD ACT Coalition Letter from ACLU et al. to U.S. Members of Congress 1 (Mar. 12, 2018), *available at* https://www.aclu.org/sites/default/files/field_document/cloud_act_coalition_letter_3-8_clean.pdf.

[42] Letter from Apple, Facebook, Google, Microsoft & Oath, to Doug Collins, Darrell Issa, Tom Marino, Hakeem Jeffries, Suzan DelBene & John Rutherford, Representatives, U.S. Congress (Feb. 6, 2018), *available at* https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-House-CLOUD-Act-020618.pdf.

[43] Daskal & Swire, *supra* note 40.

[44] Ellen Nakashima & Andrea Peterson, *The British Want to Come to America—with Wiretap Orders and Search Warrants*, WASH. POST (Feb. 4, 2016), *at* https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america–with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html?noredirect=on&utm_term=.4649759d38ea; *see also* Andrew Keane Woods, *The US-UK Data Deal*, LAWFARE (Feb. 10, 2016), *at* https://lawfareblog.com/us-uk-data-deal (arguing that "an agreement, with the right safeguards, can be seen as critical for the preserving [of] the internet as we know it, and over the long term a significant victory for privacy").

[45] Downing Testimony, *supra* note 3, at 13–14; *see also* Kadzik Letter, *supra* note 10, at 1 ("The legislative proposal is necessary to implement a potential bilateral agreement between the United Kingdom and United States.").

https://doi.org/10.1017/ajil.2018.61 Published online by Cambridge University Press

"[e]xpeditiously implementing similar agreements with the European Union and other allies. . . ."[46] British officials also voiced strong support for the CLOUD Act, with Prime Minister Theresa May stressing the "great importance of the legislation" to President Trump,[47] and U.K. Deputy National Security Advisor Paddy McGuinness testifying in support of the legislation in committee hearings in both the House of Representatives and the Senate.[48]

Despite this public support and the Act's passage, a draft of the U.S.–U.K. agreement had not been released as of May 31, 2018, and the attorney general had not submitted the necessary written certification to Congress.

## *Trump Administration Expels Russian Diplomats and Imposes Russia-Related Sanctions*

doi:10.1017/ajil.2018.59

During the spring of 2018, the Trump administration expelled sixty Russian intelligence officers and diplomats and also imposed sanctions against various Russian individuals and companies.[1] These actions responded to a range of actions attributed to Russia, including a poisoning on U.K. soil, its efforts to destabilize Ukraine, its support of the Assad regime in Syria, and various cyber activities.

On March 4, 2018, a military-grade nerve agent was used against a former Russian double agent, now a British citizen, and his daughter in the U.K. city of Salisbury.[2] British Prime Minister Theresa May attributed this act to Russia, calling it an "unlawful use of

[46] Office of Sen. Orrin Hatch Press Release, Hatch Previews CLOUD Act: Legislation to Solve the Problem of Cross-Border Data Requests (Feb. 5, 2018), *at* https://www.hatch.senate.gov/public/index.cfm/2018/2/hatch-previews-cloud-act-legislation-to-solve-the-problem-of-cross-border-data-requests [https://perma.cc/CEK2-PKBN].

[47] British Prime Minister's Off. Press Release, PM Call with President Trump: 6 February 2018 (Feb. 6, 2018), *at* https://www.gov.uk/government/news/pm-call-with-president-trump-6-february-2018 [https://perma.cc/R83W-HUFR].

[48] *See Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 15 (June 15, 2017) (statement of Paddy McGuinness, U.K. Deputy National Security Advisor); *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights Before S. Comm. on the Judiciary*, 115th Cong. (May 24, 2017, rescheduled from May 10, 2017) (statement of Paddy McGuiness, U.K. Deputy National Security Advisor).

[1] U.S. Dep't of State Press Release, Holding Russia Accountable for Its Destabilizing Behavior (Mar. 26, 2018), *at* https://www.state.gov/r/pa/prs/ps/2018/03/279552.htm [https://perma.cc/2LQF-ZY6R] [hereinafter Mar. 26 State Press Release]; U.S. Dep't of Treasury Press Release, Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity (Apr. 6, 2018), *at* https://home.treasury.gov/news/featured-stories/treasury-designates-russian-oligarchs-officials-and-entities-in-response-to [https://perma.cc/42Q7-ZG2B] [hereinafter Apr. 6 Treasury Press Release]. For an account of prior responses by the administration to Russian behavior, including other sanctions imposed earlier in the spring, see Jean Galbraith, Contemporary Practice of the United States, 113 AJIL 296 (2018).

[2] Guy Faulconbridge & Michael Holden, *Explainer: The Poisoning of Former Russian Double Agent Sergei Skripal*, REUTERS (Mar. 13, 2018), *at* https://www.reuters.com/article/us-britain-russia-explainer/explainer-the-poisoning-of-former-russian-double-agent-sergei-skripal-idUSKCN1GP2CH.