COUNCIL *on*
FOREIGN
RELATIONS

CYBER BRIEF

A New Framework for Cross-Border Data Flows

Karen Kornbluh
June 2016

This Cyber Brief is part of the Digital and Cyberspace Policy program.

The flow of data across international borders creates jurisdictional challenges, as the data itself and the person generating it may be subject to different countries' laws. International tensions result when law enforcement seeks evidence stored on a foreign server during a domestic criminal investigation or when individuals expect domestic privacy protections for data hosted abroad. Increasingly, countries have responded by imposing new requirements to store data locally, threatening cross-border data flows, which generate approximately $2.8 trillion of global gross domestic product each year. The United States should explore new avenues to prevent these restrictions on the free flow of data. Given that the majority of the world's largest Internet companies are headquartered in the United States, tensions erupt most frequently when foreign citizens' data is held by U.S. companies or stored on U.S. soil.

The United States can both raise international data privacy standards and promote the norm of the free flow of information. It can do so by building on several recent diplomatic successes, including the Privacy Shield agreement between the European Union (EU) and the United States, as well as ongoing U.S.-UK negotiations to streamline access to data in criminal cases.

The United States should act with great care to ensure its efforts raise overall privacy protections rather than subverting them. It can do so in three ways. First, the U.S. government should promote a common approach to data protection that is gaining traction through regional agreements such as the Privacy Shield and the Asia-Pacific Economic Cooperation's (APEC) privacy framework in order to lessen growing privacy concerns. Second, the United States should finally update the mutual legal assistance treaty (MLAT) system, increasing the legitimacy of legal methods for obtaining cross-border access to evidence in criminal investigations. Third, the United States should leverage its willingness to take these actions in diplomatic negotiations to seek international endorsement of the norm of the free flow of information. The time to do this is now, when increasing numbers of countries are imposing requirements that data be stored locally, also known as "forced localization," and when digital issues are on the agenda of the Group of Twenty (G20). This framework would reduce tensions between national sovereignty and the borderless Internet, on which the U.S. economy relies heavily, while strengthening respect for human rights, privacy protections, and the rule of law online.

BACKGROUND

The jurisdictional conflicts arising from cross-border data flows usually involve foreigners' data on servers belonging to U.S. companies. U.S. communication privacy law prohibits electronic communications companies from disclosing communications content except in certain situations—such as when compelled to do so in response to a U.S. warrant, court order, or subpoena—even when it is sought by a foreign country investigating a crime committed on its soil by a non-U.S. citizen. As a result, the principal recourse for foreign law enforcement is the system of MLATs, which protects the due process rights of the individual. However, U.S. procedures for complying with a request are opaque and take an average of ten months to complete.

Edward Snowden's disclosure of the extent of National Security Agency (NSA) surveillance has fueled privacy concerns from individuals whose data winds up on U.S. companies' servers. The fifteen-year-old EU-U.S. Safe Harbor agreement, under which U.S. companies transferred personal data across the Atlantic by certifying that their privacy procedures complied with EU data protection laws, was struck down by the Court of Justice of the European Union in October 2015. The court acted in response

to an Austrian student's complaint, based in part on incorrect press accounts, that personal data he provided to Facebook was readily accessible to the NSA, in violation of European privacy laws.

Fortunately, the United States has taken steps to ease these frictions. In February 2016, the European Union and United States agreed to replace Safe Harbor with Privacy Shield, which provides the European Union with assurances that data on its citizens that is transferred to the United States will be handled in accordance with EU privacy norms. In March 2016, the U.S. attorney general revealed that the United Kingdom and the United States are negotiating a deal to allow UK law enforcement agencies expedited access to data held in the United States. The United States can attempt to build on these efforts to further ease international concern about privacy and law enforcement access to data when it travels to the United States. The United States can also build on the Trans-Pacific Partnership provisions designed to protect the movement of data.

This focus of the G20 this year on digital issues is an opportunity to gain acceptance of the norm of the free flow of information. A statement in favor of such a norm would not obligate countries to remove data localization requirements, and therefore might be achievable coupled with good faith efforts on the part of the United States to ease tensions.

CHALLENGES TO A NEW FRAMEWORK

Despite these modest successes, there are considerable challenges to resolving the tension between national sovereignty and international data flows. Privacy law scholars Peter Swire and Justin D. Hemmings argue that the increased use of encryption on consumer devices leads foreign law enforcement agencies to seek access to the same data in unencrypted form, which in some cases is hosted on a server in the United States. When confronted with the dysfunction of the MLAT system, countries may attempt to compel U.S. companies to hand over data in violation of U.S. law, require that data be stored locally, or mandate backdoors to unlock encrypted devices. Therefore, increasing foreign law enforcement's access to data held by U.S. companies, if accomplished *with the appropriate safeguards*, could have the counterintuitive effect of strengthening protections. However, care should be taken not to grant access too broadly to the wrong regimes and thereby risk weakening human rights protections.

Gaining a statement of support in the G20 for the norm of the free flow of information will be challenging, despite the benefits of cross-border data flows to international collaboration and economies of scale and despite good will gestures by the United States. Concerns from individual users and foreign governments regarding the treatment of data held by U.S. companies are behind some countries' requirements that companies store personal data domestically. However, several G20 countries, notably Russia and China, have other interests in restricting data flows. Through multilateral diplomacy, the United States can explore whether it can garner enough support from countries eager for the United States to address their privacy and law enforcement concerns that a few remaining countries would be reluctant to oppose a broadly supported agreement.

RECOMMENDATIONS

In order to preserve the openness and global reach of the Internet, the United States should encourage the adoption of an international framework for increasing privacy and human rights protections while safeguarding the free flow of information.

First, the United States should, to the extent practicable, encourage countries to adopt an approach to data protection that raises privacy protections when data crosses international borders to approximate international norms or the individual's domestic laws. Successive agreements and reports, such as the revised privacy guidelines of the Organization for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation privacy framework, and the new Privacy Shield, have endorsed this approach, referred to as "interoperability." The United States should encourage broader adoption of these agreements. In addition, the U.S. Judicial Redress Act, part of Privacy Shield, grants EU citizens standing to sue the U.S. government concerning its collection of EU data. The U.S. government should add additional partners to the list of countries whose citizens can make similar claims, under the new law's provision allowing the U.S. attorney general (with the agreement of the secretaries of State, Treasury, and Homeland Security) to do so.

Second, the United States should undertake two separate reforms to address foreign law enforcement's frustration with the MLAT process, thereby discouraging attempts to circumvent the system and its due process protections. The U.S. government should expedite and simplify the MLAT process through a variety of measures such as increased funding for the Department of Justice's Office of International Affairs and the introduction of standardized, online requests, as recommended in the 2013 report by the President's Review Group on Intelligence and Communications Technologies. This would make the current system more legitimate and user-friendly without weakening its protections. In addition, the United States could allow countries with high human rights standards to join the eventual U.S.-UK agreement. Such a partnership would provide a reward for nations that respect due process and human rights. The system would safeguard against abuse by operating with stringent criteria, including those proposed by legal scholars Jennifer Daskal and Andrew K. Woods (such as the submission of targeted, particularized requests subject to robust minimization procedures and authorized by an independent adjudicator, and committing to transparency reports). Digital privacy expert Greg Nojeim has outlined additional restrictions that should also be considered, including that the crime be wholly committed in the requesting country, that the only connection to the United States should be the headquarters of the company holding the data, and that the U.S. company would not be required to release the information but would be required to notify the Department of Justice, which would ensure the information is not sought to restrict speech or undermine human rights.

Third, the United States should work to obtain G20 leaders' endorsement for the OECD's Internet policymaking principles, which include allowing cross-border information flows and respecting human rights, as well as endorsement of interoperable privacy protection, such as the OECD privacy guidelines, APEC's privacy framework, and the EU-U.S. Privacy Shield. Gaining Chinese and Russian support will be difficult, but digital issues are on this year's G20 agenda and China, as its host, is seeking deliverables, which provides the United States with some diplomatic leverage. Russia's stated ambition to join the OECD, which would require acceding to the principles, may provide additional leverage.

Recent, modest successes provide the United States with an opportunity to help resolve conflicts over privacy protections and law enforcement access to data through interoperable agreements. Forging these agreements would take flexibility on the part of the United States, but offers the opportunity to promote U.S. norms in support of an open, global, and secure Internet.

About the Author

Karen Kornbluh is the senior fellow for digital policy at the Council on Foreign Relations. She served as U.S. ambassador in Paris to the Organization for Economic Cooperation and Development, the global economic standard-setting organization. There, she spearheaded development of the first global Internet policymaking principles, launched the OECD's Gender Initiative, and co-chaired the Middle East–North Africa Women's Business Forum. Previously, she served as policy director for Barack Obama when he was in the Senate, in the Clinton administration as deputy chief of staff at the U.S. Treasury Department, and as director of the Office of Legislative and Intergovernmental Affairs at the Federal Communications Commission. Kornbluh started her career as a management consultant and has written extensively on economic, technology, and family policy in publications including the *New York Times*, *Washington Post*, *Atlantic*, and *Harvard Journal of Law and Technology*. She is currently at the Nielsen Company but the views expressed herein are her own and do not reflect the views of any organization.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

The Digital and Cyberspace Policy program addresses one of the twenty-first century's most pressing challenges: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program's fellows produce timely analysis on the most important issues in cyberspace. Cyber Briefs are short memos that offer concrete recommendations on cybersecurity, Internet governance, online privacy, and the trade of digital goods and services.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.