Proposed United States–United Kingdom Agreement on Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Countering Serious Crime, Including Terrorism

Summary

The Administration has been discussing with the United Kingdom a bilateral agreement to help resolve certain conflicting legal obligations that U.S. companies may face. These conflicts arise when British authorities investigating serious crime require U.S. companies to disclose electronic data that U.S. law prevents them from disclosing. The proposed new framework would permit British authorities to access electronic data directly from U.S. companies where the investigation targets accounts not used by U.S. persons or persons located in the United States. The United States would have reciprocal rights regarding electronic data of U.K. companies or other companies storing data in the United Kingdom, at least to the extent that our own laws reach electronic data stored abroad. If this approach proves successful, it could be replicated with other countries whose laws adequately protect related human rights and fundamental freedoms. The Administration is committed to ensuring that any such agreements protect privacy and civil liberties while facilitating more effective international law enforcement cooperation. Legislation would be required to implement any agreement and the Administration intends to work closely with Congress on a legislative framework.

The Problem

Foreign governments investigating criminal activities abroad increasingly require access to electronic evidence from U.S. companies that provide internet 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 limits the companies' ability to disclose it. Our companies may face conflicting legal obligations when foreign governments require them to disclose electronic data that U.S. law prohibits them from disclosing. This legal conflict can occur even though the request is made pursuant to lawful process in the foreign country, involves communications between foreign nationals abroad, and concerns criminal activities outside the United States with no relation to this country other than the fact that the service provider stores the data in the United States. In addition to harming our allies' efforts to investigate terrorism and other serious crimes, this puts our companies in a difficult position: either they comply with a foreign order, and risk a violation of U.S. law—or they refuse to comply, and risk a violation of foreign law.

The Mutual Legal Assistance Treaty (MLAT) process, which is an important but often labor intensive mechanism for facilitating law enforcement cooperation, must contend with the challenges posed by significant increases in the volume and complexity of requests for assistance made to the United States in the Internet age. It typically takes months to process such requests, and foreign governments often struggle to understand and comply with U.S. legal standards for obtaining data, particularly content, for use in their investigations and prosecutions. As the number of requests for electronic data

continues to grow as a result of the Internet's globalization of personal communications, governments with legitimate investigative needs face increasingly serious challenges in gaining efficient and effective access to such data. Reforming the MLAT process must remain a priority, but at the same time it is critical to find even more streamlined solutions for data held by and transmitted via Internet Service Providers.

The current situation is unsustainable. Some countries have begun to take enforcement actions against U.S. companies, imposing fines or even arresting company employees. If foreign governments cannot access data they need for legitimate law enforcement, including terrorism investigations, they may also enact laws requiring companies to store data in their territory. Such "data localization" requirements would only exacerbate conflicts of law, make Internet-enabled communications services less efficient, threaten important commercial interests, undermine privacy protections by requiring data storage in jurisdictions with laws less protective than ours, and ultimately impede U.S.-government access to data for its investigations. And as the global market for Internet-related services expands, the U.S. government will increasingly need effective and efficient access to electronic information stored or uniquely accessible abroad. Conflicts of law may increasingly pose an obstacle to such access.

The Solution

The Administration has begun negotiations with the United Kingdom to establish a new framework that would permit British authorities to access electronic data directly from U.S. companies where the investigation targets accounts not used by U.S. persons or people in the United States. The agreement would apply to orders intended to detect, prevent, investigate, or prosecute serious crimes, including terrorism and proliferation of weapons of mass destruction. It would apply to both content and non-content, and intercepts of communications as well as access to stored data. To qualify, the United Kingdom would have to agree to a number of rules designed to protect privacy and civil liberties, and a U.K. order would have to comply with U.K. law. Significantly, the agreement and implementing legislation would only serve to remove U.S. legal barriers to our companies' ability to comply with U.K. orders subject to the agreement. It would not require our companies to comply with a U.K. order; they would remain free to challenge an order or contest U.K. jurisdiction in U.K. courts. Moreover, if a company believed that an order fell outside the scope of the agreement and it could not resolve the issue with the United Kingdom, the company could raise that issue with the U.S. government. If the U.S. government concludes that a U.K. order does not properly fall within the scope of the agreement, it could "veto" the agreement's application to the order, in which case the domestic U.S. legal bar would remain in place. In cases where U.S. law permits us to compel the production of data that may be stored abroad, the United States would obtain reciprocal rights with regard to access to data of U.K. companies or other companies storing data in the United Kingdom, subject to reciprocal restrictions. The agreement would not be the exclusive mechanism for either government

to obtain access to cross-border data; other mechanisms such as MLATs would remain in place.

The agreement, and any others that the Executive Branch might consider having with other countries, would include numerous provisions designed to protect privacy and civil liberties, including the following:

- The United Kingdom may not intentionally target a U.S. person or a person located in the United States, and must adopt targeting procedures designed to meet this requirement;
- The United Kingdom may not target a non-U.S. person located outside the United States if the purpose is to obtain information concerning a U.S. person or a person located in the United States;
- The United Kingdom may not issue an order if a purpose is to obtain information to provide to the U.S. government, nor may the U.K. government be required to share any information produced with the U.S. government;
- The United Kingdom must adopt appropriate procedures to minimize the acquisition, retention, and dissemination of any information obtained concerning U.S. persons, and such procedures must be approved by the U.S. government;
- The United Kingdom may issue orders only for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;
- The United Kingdom may not issue orders requiring the production of information in bulk;
- The United Kingdom must issue orders in compliance with its law;
- The United Kingdom may not issue orders that would facilitate infringements upon freedom of speech; and
- The United Kingdom must agree to periodic review of its compliance with the terms of the agreement by the U.S. government, and appropriate transparency measures.

Under the legislative framework contemplated by the Administration, the Executive Branch could only enter into agreements of this kind upon certifying to Congress that the United Kingdom (or another foreign government, in the case of any other agreement) had made and was prepared to implement these substantial commitments. The Executive Branch would also have to certify to Congress that the foreign government's law governing orders includes requirements for sufficient cause, particularity, legality, and severity regarding the conduct under investigation, and that the foreign government's domestic laws and practices meet certain baseline standards related to rule of law and human rights. Finally, the Executive Branch would be required to notify Congress and conduct consultations in advance of making such determinations and entering into any

such agreements. Periodic renewals of such determinations could also be required in order to maintain an agreement.

Benefits of Such Agreements to the United States

There are multiple benefits that such agreements would have for important U.S. interests:

- Removing barriers and conflicts for U.S. businesses. The proposed agreement with the United Kingdom and others like it would help U.S. companies avoid potential conflicts of law and enforcement actions that could jeopardize their ability to continue to market their services overseas. U.S. companies have repeatedly emphasized that such conflicts are a serious problem for them.
- Protecting U.S. interests and citizens. The agreement would strengthen U.S. public safety by supporting U.K. efforts at combating transnational threats, including international terrorism, proliferation and transnational crime. It also would help the United Kingdom fight other serious crime in the United Kingdom, some of which may be directed against U.S. persons. If similar agreements are negotiated with other allies, these benefits would be magnified.
- Ensuring reciprocal access. The agreement would secure reciprocal access for U.S. authorities to electronic data in the U.K. (and potentially in other countries that conclude similar agreements with the United States) to the extent it is within the reach of U.S. law. This access will become more important if more U.S. companies store data in the United Kingdom or elsewhere abroad or if foreign companies gain a larger share of the global market.
- Reducing data localization incentives. By giving the United Kingdom more effective access to data in the United States, the agreement lowers U.K. incentives to impose data localization requirements. Similar agreements with other rights-respecting countries could help counter calls for data localization elsewhere around the world.
- Reducing MLAT burden. The agreement would lessen the burden on U.S. government resources dedicated to processing incoming MLAT requests from the United Kingdom (and potentially other countries), and would allow the United States to respond to all other MLAT requests more efficiently.
- Encouraging improvement of global privacy protections. The promise of future agreements with other countries could serve as an incentive to encourage those countries to improve their substantive and procedural protections for privacy, or related human rights and fundamental freedoms, in order to be eligible for an agreement. This could result in improvements in foreign laws governing access to electronic data or on other issues related to privacy and civil liberties. It could also encourage them to resolve other bilateral law enforcement or information sharing issues with the United States.