Cover Sheet

Statement of David S. Kris
Before the Committee on the Judiciary, U.S. House of Representatives,
Hearing on International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests
February 25, 2016

Statement of David S. Kris
Before the Committee on the Judiciary, U.S. House of Representatives,
Hearing on International Conflicts of Law Concerning Cross Border Data Flow and
Law Enforcement Requests
February 25, 2016

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, thank you for inviting me to testify. I am a former Department of Justice official and the co-author of a treatise on national security investigations and prosecutions, and I am testifying in my individual capacity, not as a representative of any other party. My testimony is drawn from two papers that I recently wrote: *Preliminary Thoughts on Cross-Border Data Requests*, and *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, both of which are available at www.lawfareblog.com. These papers cover in more detail, with appropriate citations and support, the points set out below.

1. Today, for reasons both technological and political, there are growing conflicts between U.S. and foreign laws regulating production of data in response to governmental surveillance directives. These conflicts arise where one government's laws compel the production of data, and another government's laws forbid that production. From the U.S. perspective, the conflicts typically present in two main forms.

First, major U.S. electronic communication service providers face escalating pressure from foreign governments, asserting foreign law, to require production of data stored by the providers in the United States, where the production would violate U.S. law. For example, the United Kingdom's Data Retention and Investigatory Powers Act 2014 (DRIPA) explicitly authorizes the UK to compel production of data from anyone providing a communications service (such as email) to customers in the UK, even if the data in question are stored abroad. But the U.S. Stored Communications Act (SCA) generally forbids production of certain data (including the contents of email) stored in the U.S., and does not contain an exception for production of data in response to a UK directive.

Second, at the same time, foreign governments also are increasingly likely to enact laws forbidding production of locally-held data in response to U.S. (and other) demands for its production, and also to enact laws requiring certain data to be held locally, creating a form of reciprocal pressure. Currently pending in the Second Circuit is a case in which the U.S. government is relying on the SCA to compel Microsoft to produce email stored in Ireland; Microsoft is resisting on the ground that the SCA cannot compel production of data stored abroad; and the Government of Ireland has filed an amicus brief supporting Microsoft and asserting its sovereignty, but conceding that it is "incumbent upon Ireland to acknowledge" that "there may be circumstances in which an Irish court would order the production of records from an Irish entity on foreign soil," perhaps even if "execution of the order would violate the law of the foreign sovereign."

In this environment, the same action in response to a surveillance directive may be at once both legally required by one government's laws, and legally forbidden by another's. Although this problem is not unprecedented – with antecedents in cases involving U.S. grand jury subpoenas for bank records held in foreign countries with strict bank secrecy laws – the conflicts have been increasing lately in frequency and intensity. That is due to technological and political factors, including the growing size, speed and use of the Internet and other data networks; greater use of remote data storage (e.g., the cloud); the Snowden disclosures and resulting suspicion of U.S. surveillance practices in Europe; the U.S.

government's reaction to those disclosures by decreasing the scope and increasing the transparency of certain of its surveillance practices; the increased use of encryption; the rise of the Islamic State of Syria and the Levant (ISIL); and European governments' reaction to ISIL's rise by increasing the scope of their own surveillance.

International agreements, and appropriate domestic legislation, could help reduce conflicts and rationalize surveillance rules to promote international commerce, law enforcement, protection of civil liberties, and the worldwide rule of law. The simplest approach in concept would be to remove or override domestic legal prohibitions on disclosure, where desired, in response to certain types of favored foreign production directives. This would probably begin in a bi-lateral setting with the UK, and could expand from there. As a matter of U.S. law, it would not be difficult technically, although it might be very challenging politically, to make the necessary amendments. There certainly are other ways to approach the issue, including reforms to our various Mutual Legal Assistance Treaties or the processes for implementing them. Absent some new international approach, however, we face the prospect of an increasingly chaotic and dysfunctional system for cross-border data requests that benefits no one.

2. Although many of the challenges in this area arise in connection with ordinary law enforcement, I should highlight two related gaps in U.S. law regulating foreign intelligence surveillance. First, whatever the merits of Microsoft's argument in the case discussed above, there is no real doubt that it would prevail if the U.S. government sought to compel production of email stored in Ireland under the Foreign Intelligence Surveillance Act (FISA), if the target were either a U.S. person (in any location) or a person (of any nationality) located in the United States. That is because traditional FISA searches may only occur in the United States; traditional FISA electronic surveillance applies to stored data only when the surveillance device is used in the United States; Section 702 of the FISA Amendments Act (FAA) applies only to non-U.S. persons located abroad; Section 703 applies only when the surveillance is conducted in the United States; and Section 704 (which applies to U.S. persons abroad) cannot be used to compel assistance from a provider. In short, unless the provider voluntarily repatriates the stored email, its production cannot be compelled under FISA. This is a potentially significant shortfall in the statute, particularly as data become more and more mobile, subject to being stored in any location, or even fragmented and stored in several locations at once.

A second possible gap concerns the situation in which all parties to a communication are located abroad, but the communication transits a wire in the United States. In that situation, it has long been the case that the U.S. government generally cannot get a FISA Court order to compel the assistance of the provider that owns the wire. Unless it has a valid target under FAA Section 702 (a non-U.S. person located abroad), the most the government can do is assure the provider, in the form of a certification from the Attorney General, that it may lawfully cooperate, but not that it must do so. If a provider refuses, the government has very little recourse. Today, with providers more recalcitrant than they have been, voluntary assistance may not be forthcoming.

These two and several other important issues in the field of foreign intelligence surveillance (addressed in the papers cited above) should, in my opinion, be considered by Congress soon.

Again, thank you very much for inviting me to testify and for considering my views. I am happy to answer any questions.