Prepared Statement by Senator Chuck Grassley of Iowa
Chairman, Senate Judiciary Committee
Subcommittee on Crime and Terrorism
Hearing on "Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights"
May 24, 2017

Today's hearing will help inform this Subcommittee of the Senate Judiciary Committee about a few of the most recent developments concerning possible reforms to the Electronic Communications Privacy Act.

In 1986, Congress enacted ECPA to both protect the privacy of Americans' electronic communications and provide law enforcement with a means to access those communications and related records in certain circumstances. However, dramatic changes in the use of communications technology have occurred since then.

Two of those changes are related to today's hearing. First, American companies offering internet services to customers across the globe are increasingly choosing, for business purposes, to store email and other data outside the United States, which created the foundation for a significant legal challenge to the current ECPA regime. And second, the increasing use of email by all manner of criminals -- terrorists, drug dealers, child predators, and fraudsters -- means that law enforcement access to this data is increasingly essential to solving crimes and protecting lives and property, whether here or abroad.

As these trends were accelerating last year, a three-judge panel of the Second Circuit held that an ECPA warrant doesn't permit the Department of Justice to obtain email that an American company chooses to store outside the United States. Put another way, even though in that case the government had met the highest level of privacy protection ordinarily required by the Fourth Amendment – probable cause of a crime demonstrated to a neutral judge – under the Court's interpretation of the statute, the business decisions of an American company may serve to place important evidence outside the purview of American law enforcement. Under the Court's reasoning, this is so, even if the crime being investigated took place in America, with American victims. Certainly, this decision placed the issue of data stored across borders squarely on Congress's doorstep.

Also last year, the Department of Justice sent to Congress proposed legislation to implement the so-called "U.S.-U.K." agreement. This agreement would permit British law enforcement to obtain the email data of British citizens held by American companies if certain enhanced privacy protections are satisfied under British law.

Of course, this kind of data held by American companies is also valuable to law enforcement authorities abroad. Electronic communications data can help solve a murder in London just as easily as in New York. But in considering whether to implement such agreements, Congress

needs to closely consider what sorts of additional privacy standards or processes it would require of foreign governments.

These aren't easy questions, and there aren't easy answers. Certainly, we all want law enforcement, in the United States especially, to have the tools to solve crimes and assist victims.

But we also need to ensure that privacy interests are preserved, and that American companies remain the most innovative and competitive in the world. I hope today's hearing kicks off a conversation in the Senate about how best to reconcile all of these important interests. Thank you, Senators Graham and Whitehouse, for holding this important hearing.

-30-