U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D. C. 20530

NOV 1 3 2017

The Honorable Lindsey Graham
Chairman
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance of Deputy Assistant Attorney General Brad Wiegmann before the Subcommittee on May 24, 2017, at a hearing entitled "Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights."

Thank you for the opportunity to present our views. Please do not hesitate to contact this office if we may be of additional assistance to you. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Stephen E. Boyd
Assistant Attorney General

Enclosure

cc: The Honorable Sheldon Whitehouse
Ranking Member

RESPONSES OF
BRAD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL

TO QUESTIONS FOR THE RECORD
ARISING FROM A HEARING
BEFORE THE
SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ENTITLED
"LAW ENFORCEMENT ACCESS TO DATA STORED ACROSS BORDERS:
FACILITATING COOPERATION AND PROTECTING RIGHTS"

MAY 24, 2017

Questions from Senator Graham:

1. **Is the Second Circuit's decision in the *Microsoft/Ireland* case consistent with the United States' obligations under the Budapest Convention on Cybercrime? Why?**

No. The Second Circuit's interpretation of the Stored Communications Act ("SCA") in the *Microsoft/Ireland* case has rendered the United States out of compliance with its obligations under the Budapest Convention on Cybercrime.

Article 18.1.a of the Budapest Convention on Cybercrime (Cybercrime Convention) provides that "[e]ach Party *shall* adopt such legislative and other measures as may be necessary to empower its competent authorities to order . . . a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium[.]" Cybercrime Convention, Art. 18.1.a (emphasis added). The official Explanatory Report for the Cybercrime Convention indicates that Article 18.1.a's use of the term "possession or control" in paragraph 1(a) of Article 18 "refers to physical possession of the data concerned in the ordering Party's territory, *and situations* in which the data to be produced *is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory* . . . ." *See* Explanatory Report ¶ 173 (emphasis added). The instruction clearly focuses on the location of persons with control over data, such as Microsoft as a corporate "person," not on the location of data.

Prior to the *Microsoft/Ireland* case, the prevailing interpretation of the SCA's reach—that it could be used to require an Internet Service Provider (ISP) in the U.S. to produce information within its possession, custody, or control regardless of where the data was located—was consistent with the United States' obligations under Article 18.1.a. Action is urgently needed to ensure United States compliance with its obligations under the Convention.

2. Is the nationality-based approach taken in the *International Communications Privacy Act* consistent with the United States' obligations under the Budapest Convention on Cybercrime? Why?

No. Article 18.1.a's requirement is premised entirely on whether the "person" (which includes an ISP) being ordered to produce information is within the signatory's territory and whether that person has "possession or control" over the information at issue. *See* Cybercrime Convention, Art. 18.1.a; Explanatory Report ¶ 173. The nationality of the subscriber at issue is not a factor. Indeed, Article 18.1.b, which deals with subscriber information held by a service provider, also does not account for a subscriber's nationality; instead, it applies to any subscriber of a service "offered in the ordering Party's territory." *See* Explanatory Report, ¶ 173; *see also* Cybercrime Convention, Art. 18.1.b; Cybercrime Convention Committee (T-CY) Guidance Note #10 at 5 ("Article 18.1.b is to be applied with respect to any service provider offering its services in the territory of the Party.").

Moreover, the foreign notice provisions in ICPA are also inconsistent with the confidentiality obligations the United States has undertaken in more than 80 bilateral Mutual Legal Assistance Treaties (MLATs) and various multilateral conventions. Upon the request of the treaty partner, these obligations require the United States to exercise best efforts to protect the integrity of a foreign investigation by keeping it confidential.

Confidentiality is critically important in the MLAT context. The ability of the U.S. to provide assistance subject to confidentiality ensures that U.S. requests to treaty partners similarly are protected from disclosure, especially to the subjects of the investigation. To the extent that an alleged conflict of law arises between the country of nationality of a subscriber (or the country of the location of foreign-stored data) and a U.S. request for production of foreign-stored data, made at the behest of a foreign treaty partner, ICPA's notice requirement would not be consistent with U.S. obligations to its treaty partners who request assistance subject to confidentiality. Thus, the notice provisions of ICPA implicate U.S. obligations under the Cybercrime Convention *and* other U.S. treaty obligations.

3. Why has the Administration proposed a congressional-executive agreement instead of a treaty for implementing reciprocal access by certified countries to data stored across borders? Does such an approach raise any constitutional concerns?

As stated in the Administration's letter of May 24, 2017 transmitting the proposal, legislation would be needed to provide authority to implement the proposed international agreements. Relying on legislation to authorize such agreements is consistent with past practice in a number of other areas and would allow the United States to put such agreements into place quickly and efficiently. It would also avoid the need for separate approvals of substantially similar agreements with multiple countries that conform to parameters enacted by Congress through legislation. Congress would play a substantial role by setting a robust baseline for

privacy and civil liberty protections that a country must meet to qualify for any agreement, as well as the parameters that would govern operation of an agreement, without the need for repetitive and time-consuming individual review.

The Administration's proposal would also provide Congress with advance notice of any proposed executive agreement and impose a waiting period before any such agreement entered into force. Congress would thereby have the ability to express concerns about any agreement before the United States becomes bound by it.

Congressional-executive agreements are valid and constitutional. "The constitutionality of such 'Congressional-Executive agreements' is firmly established." *Validity of Cong.-Exec. Agreements That Substantially Modify the United States' Obligations Under an Existing Treaty*, 20 U.S. Op. Off. Legal Counsel 389, 398 (1996); *accord Treaties and Other International Agreements: The Role of the United States Senate*, S. Prt. No. 106-71, at 5, 106th Cong., 2d Sess. 5 (2001) ("The constitutionality of this type of agreement seems well established and Congress has authorized or approved them frequently.") ("S. Prt. 106-71"); *see also, e.g., American Ins. Ass'n v. Garamendi*, 539 U.S. 396, 415 (2003) ("[O]ur cases have recognized that the President has authority to make 'executive agreements' with other countries, requiring no ratification by the Senate ... this power having been exercised since the early years of the Republic"); *United States v. Belmont*, 301 U.S. 324, 330 (1937) ("[A]n international compact ... is not always a treaty which requires the participation of the Senate"); *Field v. Clark*, 143 U.S. 649, 691 (1892) ("[I]n the judgment of the legislative branch of the government, it is often desirable, if not essential . . . to invest the president with large discretion in matters arising out of the execution of statutes relating to trade and commerce with other nations.").

Several notable congressional-executive agreements have withstood judicial challenge in recent decades. *See, e.g., Made in the USA Found. v. United States*, 242 F.3d 1300 (11th Cir. 2001) (affirming dismissal of constitutional challenge to North American Free Trade Agreement and related congressional-executive agreements on justiciability grounds, recognizing that "the Supreme Court has long since recognized the power of the political branches to conclude international 'agreements that do not constitute treaties in the constitutional sense'" quoting *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 318 (1936)); *Ntakirutimana v. Reno*, 184 F.3d 419, 424-27 (5th Cir. 1999) (confirming legality of extradition pursuant to executive agreement between United States and International Criminal Tribunal for Rwanda and implementing statute); *United States v. Walczak*, 783 F.2d 852 (9th Cir. 1986) (giving full force of law to US-Canada executive agreement on airport pre-clearance screening impliedly authorized by Congress). Indeed, the practice "dates from the earliest days of the Nation's constitutional history":

> Over the years, Congress has authorized or sanctioned additional agreements concerning a wide variety of subjects including, inter alia, the protection of intellectual property rights, acquisition of territory, national participation in various international

> organizations, foreign trade, foreign military assistance, foreign economic assistance, atomic energy cooperation, and international fishery rights.

S. Prt. 106-71 at 78-79 (footnotes omitted). For these reasons, the use of a congressional-executive agreement in lieu of a treaty would not raise constitutional concerns.

4. Would the United States be able to enjoy the reciprocal benefits of the Administration's proposal for implementing reciprocal access by certified countries to data stored across borders if the Second Circuit's decision in the *Microsoft/Ireland* case were the controlling rule?

No. Wherever the *Microsoft/Ireland* decision is in effect, the United States will likely be blocked from obtaining the direct, reciprocal benefits of bilateral data access agreements. Under the Administration's proposed international framework, no new authority to obtain access to data abroad would be conferred on either the United States government or its foreign partners. Rather, each country would be required to rely on its own domestic law to compel production of data stored in the other country. Under the *Microsoft/Ireland* ruling, the United States is prohibited from using SCA warrants to compel the production of data stored abroad. With no other clear alternative available, the United States would have no established authority to obtain foreign-stored data and likely would be unable to enjoy the reciprocal benefits of any bilateral agreement. Accordingly, although there are still important interests that would be served by enacting the Administration's proposed international framework – such as reducing the risk of conflicts of law faced by U.S. communications providers – direct, reciprocal benefits for the United States of bilateral data access agreements may be unavailable unless and until the *Microsoft/Ireland* decision is successfully challenged or not followed by other courts.

This is why the Administration has proposed a simple legislative fix to reverse the decision, while dealing with any potential conflicts of law through the international framework.

5. Why does the Administration's proposal for implementing reciprocal access by certified countries to data stored across borders require the certified country to not target U.S. persons, while the Administration's proposal allowing ECPA warrants to reach extraterritorially does not at all depend on nationality? Why should the United States seek to prevent access to data relating to a U.S. person by a certified country that has jurisdiction over a crime committed by that U.S. person?

The Administration's proposal does not and could not limit our foreign partners' *authority* under their domestic law to compel access to data of U.S. persons in their criminal investigations. Rather, it seeks to address the potential conflict of laws that can result if U.S. law bars disclosure of data in response to a valid foreign order. In that circumstance, the Administration believes it is appropriate to create a new exception to the U.S. legal bars on disclosure when a qualifying foreign government seeks data of non-U.S. persons outside the

United States and the agreement applies. In other words, under the Administration's approach, the nationality of the target is not relevant to the U.S. or another country's assertion of criminal investigative authority, but it can be a relevant factor in whether the country chooses to apply its privacy laws to bar disclosure of data.

The Administration's approach to these issues maximizes the protection of U.S. persons. Authorizing U.S. courts to issue warrants requiring the disclosure of data stored by providers outside the United States recognizes the long-standing, internationally-accepted principle that every nation has the right to compel providers within its jurisdiction to produce data. This principle reflects the essential duty of the United States to protect its citizens and individuals within its borders from serious crime and terrorism threats, even when they arise from overseas or involve foreign nationals. At the same time, the Administration's proposal for reciprocal access to data does not affect legal protections under U.S. law for the privacy of U.S. persons; *i.e.*, it does not remove any U.S. legal bar on production of certain data where foreign countries are targeting Americans or others located here, subject to the exceptions already present in ECPA. This approach reflects that the United States' interest in applying its privacy laws is greatest when the data is stored within our borders *and* relates to our nationals or others living here.

6. What other areas of law predicate the availability of investigative or discovery tools on a person's nationality instead of whether there is jurisdiction over the relevant conduct, such as criminal activity?

Although there are instances in which U.S. law affords greater protections to U.S. nationals and residents than to foreign nationals residing abroad, I am unaware of any U.S. law that restricts the use of investigative tools based on the foreign nationality of the target.

For example, U.S. statutes relating to wiretapping suspected criminals who are foreign citizens, using search warrants to search their houses, or using subpoenas to obtain their medical or financial records, do not give special rights or protections to foreign citizens. A requirement to provide foreign governments with notice and an opportunity to object prior to using an investigative technique to gather evidence in an investigation involving their nationals is without precedent, even in the cross-border context. For example, if we were to send a request pursuant to an MLAT to Country A, for information about a citizen of Country B, notice would not be provided to Country B – indeed, MLAT treaties generally require Country A to keep such requests confidential. These are standard international practices; I am aware of no other country's law that limits the use of investigative authorities against foreign citizens.

7. How would a thirty-day delay in the warrant application and execution process impact a variety of different investigations?

Investigations involving electronic evidence cover a large number and wide variety of Federal criminal investigations, from organized crime and drugs to violent crime and terrorism to

intellectual property crime, cybercrime, child exploitation, and fraud. State, local, and tribal police officers similarly require electronic evidence to solve almost every category of crime that they investigate.

Speed is essential when obtaining electronic evidence in criminal cases. Electronic evidence is often stored only for short periods of time by providers (both domestically and abroad), and suspects generally have the ability to destroy such evidence quickly and completely. Consequently, it is crucial that the government be able to proceed quickly in its investigation, so that it can issue preservation requests or search warrants or take other necessary measures to preserve and acquire electronic evidence.

The ability to quickly obtain electronic evidence serves a crucial public safety purpose. For example, in one investigation, officers identified an account at a U.S. provider being used by a person located outside the United States who was conspiring with Americans to trade images of ongoing sexual abuse of American infants and toddlers. The investigation of that account led directly to the rescue of American children from their abusers and the prosecution of child sex offenders. Imposing a thirty-day delay period to collect information necessary for execution of a warrant on the relevant account would have slowed the investigation and likely caused the children to suffer additional abuse.

When criminals act from or through foreign locations, law enforcement may have to collect data from more than one foreign location, basing subsequent legal process on the information learned from productions under prior process. Thus, any delay will be cumulative and would allow crimes to continue while investigation continues. This delay would create an even greater risk that evidence will be destroyed before it can be collected and used, for example, to identify the perpetrators.

For these reasons, the SCA currently imposes no statutory delays on the government's ability to gain evidence via search warrant. Adding a thirty-day delay would likely close down productive investigative leads and significantly harm law enforcement's ability to bring criminals to justice. A thirty-day delay imposed as part of the application and execution process could create cascading delays, ultimately resulting in months-long waits for evidence critical to public safety or justice.