



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 15, 2016

The Honorable Joseph R. Biden
President
United States Senate
Washington, DC 20510

Dear Mr. President:

On behalf of the Administration, I am pleased to present for the consideration of the Congress a legislative proposal that would help resolve potential conflicting legal obligations that U.S. electronic communications service providers (“service providers”) may face when required to disclose electronic data by foreign governments investigating serious crime, including terrorism. The legislative proposal is necessary to implement a potential bilateral agreement between the United Kingdom and the United States that would permit U.S. companies to provide electronic data in response to U.K. orders targeting non-U.S. persons located outside the United States, while affording the United States reciprocal rights regarding electronic data of companies storing data in the United Kingdom. Because this legislative proposal would require amendments to the Electronic Communications Privacy Act (ECPA), one potential avenue for consideration of the proposal would be in the context of current ECPA reform efforts.

Foreign governments investigating criminal activities abroad increasingly require access to electronic evidence from U.S. companies that provide electronic 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, including ECPA, 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 violating 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 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 potential bilateral agreement with the United Kingdom and the Administration's legislative proposal would not only resolve legal conflicts for communications service providers located in the United Kingdom and the United States and promote and protect the global free flow of information, it would establish a framework and standards that could be used to reach similar agreements with other countries whose laws provide robust protection of human rights, privacy, and other fundamental freedoms. It could thereby increase protections for privacy and civil liberties globally, as countries seeking to qualify for such agreements would need to demonstrate that their legal systems meet these requirements.

The legislative proposal achieves these priorities by requiring the Attorney General, with the concurrence of the Secretary of State, to determine and certify to Congress that foreign partners have met obligations and commitments designed to protect privacy and civil liberties. Orders issued by the foreign government must be subject to review or oversight by a court, judge, magistrate, or other independent authority. Significantly, foreign orders covered by this legislation and the agreements it would authorize would not be permitted to target U.S. persons wherever they are located or persons located in the United States. Procedures and oversight would be required to ensure that this rule is followed. Moreover, the Administration would be required to notify Congress prior to making the required determinations and entering into any agreements.

In order for the United States to receive reciprocal benefits from such agreements, U.S. law must authorize law enforcement to obtain electronic data located abroad. Yesterday, the United States Court of Appeals for the Second Circuit held in *Microsoft Corp. v. United States* that section 2703 of ECPA does not authorize our courts to issue and enforce warrants served on U.S. providers to obtain electronic communications stored abroad. If this decision stands, or is

extended to other parts of the country, the U.S. would not have, under 2703, access to data necessary to advance important U.S. investigations that protect the safety of Americans and could not obtain reciprocal benefits from other countries. The Administration intends to promptly submit legislation to Congress to address the significant public safety implications of the *Microsoft* decision. This will be a necessary addition to the proposal that we are submitting today.

In sum, the proposed legislation would provide numerous benefits to the United States, including: 1) removing barriers and conflicts for U.S. businesses; 2) protecting U.S. interests and citizens and enhancing public safety; 3) ensuring reciprocal access to data for U.S. investigations; 4) reducing data localization incentives; 5) reducing the mutual legal assistance burden on U.S. government resources; and 6) encouraging improvement of global privacy protections. We urge Congress to work with the Administration to pass legislation that would allow the United States to enter into and implement bilateral agreements that would achieve these important objectives.

Sincerely,


Peter J. Kadzik
Assistant Attorney General

Enclosures

**Legislation to Permit the Secure and Privacy-Protective Exchange of
Electronic Data for the Purposes of Combating Serious Crime
Including Terrorism**

Section 1: Short Title.

This Act may be cited as the “___.”

Section 2: Congressional Findings and Purpose

The Congress finds the following:

- (1) Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism.
- (2) Foreign governments increasingly seek access to electronic data held by communications-service providers in the United States for such purposes, and the United States government likewise seeks such access to electronic data held abroad.
- (3) Communications-service providers face potential conflicting legal obligations when a foreign government orders production of electronic data that United States law may prohibit providers from disclosing.
- (4) Foreign law may create similar conflicting legal obligations when the United States government orders production of electronic data that foreign law prohibits communications-service providers from disclosing.
- (5) International agreements provide a mechanism for resolving these potential conflicting legal obligations where the United States and the relevant foreign government share a common commitment to the rule of law and the protection of privacy and civil liberties.
- (6) The purpose of this Act is to authorize and to provide authority to implement such international agreements to resolve potential conflicting legal obligations arising from cross-border requests for the production of electronic data where the foreign government targets non-U.S. persons outside the United States in connection with the prevention, detection, investigation, or prosecution of serious crime.

Section 3: Amendments to Current Communications Laws.

(a) Chapter 119 of Title 18, United States Code, is amended by adding:

- (1) A new subsection 2511(2)(j) as follows:

“It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX.”;

and

(2) Replacing subsection 2520(d)(3) as follows:

“a good faith determination that section 2511(3), 2511(2)(i), or 2511(2)(j) of this title permitted the conduct complained of;”

(b) Chapter 121 of Title 18, United States Code, is amended by adding:

(1) A new subsection 2702(b)(9) as follows:

“to a foreign government pursuant to an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX.”;

(2) A new subsection 2702(c)(7) as follows:

“to a foreign government pursuant to an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX.”;

and

(3) Replacing subsection 2707(e)(3) as follows:

“a good faith determination that section 2511(3), section 2702(b)(9), or section 2702(c)(7) of this title permitted the conduct complained of;”

(c) Chapter 206 of Title 18, United States Code, is amended by:

(1) Adding to the end of subsection 3121(a) as follows:

“or an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX.”;

(2) Replacing subsection 3124(d) as follows:

“No cause of action against a provider disclosing information under this chapter.—No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter, request pursuant to section 3125 of this title, or an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX.”

and

(3) Replacing subsection 3124(e) as follows:

“Defense.—A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, a statutory authorization, or a good faith determination that the conduct complained of was permitted by an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX, is a complete defense against any civil or criminal action brought under this chapter or any other law.”

Section 4: Executive Agreements on Access to Data by Foreign Governments.

Chapter ___ of Title 18, United States Code, is amended by adding a new section XXXX as follows:

“(a) An executive agreement governing access by a foreign government to data subject to Chapters 119, 121, and 206 of this Title shall satisfy this section if the Attorney General, with the concurrence of the Secretary of State, determines and certifies to Congress that:

(1) The domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement, provided that such a determination under this section take into account, as appropriate, credible information and expert input, and that the factors to be considered in making such a determination include whether the foreign government:

(i) has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated through accession to the Budapest Convention on Cybercrime, or through domestic laws that are

consistent with definitions and the requirements set forth in Chapters I and II of that Convention;

(ii) demonstrates respect for the rule of law and principles of non-discrimination;

(iii) adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights (including but not limited to protection from arbitrary and unlawful interference with privacy; fair trial rights; freedoms of expression, association and peaceful assembly; prohibitions on arbitrary arrest and detention; and prohibitions against torture and cruel, inhuman, or degrading treatment or punishment);

(iv) has clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective of oversight of these activities;

(v) has sufficient mechanisms to provide accountability and appropriate transparency regarding the government's collection and use of electronic data; and

(vi) demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet.

(2) The foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement; and

(3) The agreement requires the following with respect to orders subject to the agreement:

(i) The foreign government may not intentionally target a United States person or a person located in the United States, and must adopt targeting procedures designed to meet this requirement;

(ii) The foreign government may not target a non–United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States;

(iii) The foreign government may not issue an order at the request of or to obtain information to provide to the United States government or a third-party government, nor shall the foreign government be required to share any information produced with the United States government or a third-party government;

(iv) Orders issued by the foreign government must be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

(v) Orders issued by the foreign government must identify a specific person, account, address, or personal device, or any other specific identifier as the object of the Order;

(vi) Orders issued by the foreign government must be in compliance with the domestic law of that country, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law;

(vii) Orders issued by the foreign government must be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;

(viii) Orders issued by the foreign government must be subject to review or oversight by a court, judge, magistrate, or other independent authority;

(ix) Orders issued by the foreign government for the interception of wire or electronic communications, and any extensions thereof, must be for a fixed, limited duration; interception may last no longer than is reasonably necessary to accomplish the approved purposes of the order; and orders may only be issued where that same information could not reasonably be obtained by another less intrusive method;

(x) Orders issued by the foreign government may not be used to infringe freedom of speech;

(xi) The foreign government must promptly review all material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those trained in applicable procedures;

(xii) The foreign government must segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or seriously bodily harm to any person;

(xiii) The foreign government may not disseminate the content of a communication of a U.S. person to U.S. authorities unless the communication (a) may be disseminated pursuant to Section 4(a)(3)(xii) and (b) relates to significant harm, or the threat thereof, to the United States or U.S. persons, including but not limited to crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud;

(xiv) The foreign government must afford reciprocal rights of data access to the United States government;

(xv) The foreign government must agree to periodic review of its compliance with the terms of the agreement by the United States government; and

(xvi) The United States government must reserve the right to render the agreement inapplicable as to any order for which it concludes the agreement may not properly be invoked.

(b) A determination or certification made under subsection (a) shall not be subject to judicial or administrative review.

(c) The Attorney General shall provide notice to the judiciary and foreign affairs committees of the Senate and House 60 days prior to making a determination under subsection (a) of his intent to do so. Any determination or certification under subsection (a) regarding an executive agreement under this section and any termination of such an agreement, shall be published in the Federal Register as soon as is reasonably practicable.

(d) The Attorney General, with the concurrence of the Secretary of State, shall renew a determination under subsection (a) every five years. In the absence of such a renewal, the agreement will no longer satisfy this section.

(e) As used in this section, "United States person" means a citizen or national of the United States, an alien lawfully admitted for permanent residence (as

defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence; or a corporation which is incorporated in the United States.”

Section 5: Rule of Construction.

Nothing in this Act shall be construed to preclude any foreign authority from obtaining assistance in a criminal investigation or prosecution pursuant to Section 3512 of Title 18, United States Code, Section 1782 of Title 28, United States Code, or as otherwise provided by law.

Section-by-Section Analysis of Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism

Currently, U.S. electronic communications service providers face potentially conflicting legal obligations when a foreign government serves them with legal process requiring the production of electronic data that U.S. law may prohibit them from acquiring or disclosing. The proposed legislation amends Title III of the Omnibus Crime Control and Safe Streets Act (the Wiretap Act), the Stored Communications Act (SCA), and Chapter 206 of Title 18 (the Pen/Trap Statute) to allow service providers to intercept, access, and disclose communications content and metadata in response to an order from a foreign government, if that order is pursuant to an executive agreement that the Attorney General, with the concurrence of the Secretary of State, has determined, and certified to Congress, meets several statutory conditions. Among these conditions is the requirement that the foreign order not target any U.S. person or any person located in the United States. In addition, the Attorney General must certify that the law of the foreign government provides robust protections for privacy and civil liberties. The legislation also provides a complete bar to civil and criminal liability for violations of the statutes if the providers acted in good faith reliance on such foreign orders, in parallel to existing provisions of law establishing such liability protection for good faith reliance on U.S. orders.

Section 2 sets forth congressional findings and the purpose of the proposed legislation—in particular, to authorize and to provide authority to implement executive agreements that resolve potential conflicting legal obligations arising from cross-border requests for the production of electronic data where a foreign government targets non-U.S. persons outside the United States in connection with the prevention, detection, investigation, or prosecution of serious crime, if that foreign government and the United States share a common commitment to the rule of law and the protection of privacy and civil liberties.

Subsection 3(a)(1) amends the Wiretap Act by adding an additional exception to the general prohibition on accessing real-time wire or electronic communications. The exception permits interception and disclosure to respond to a foreign order made pursuant to an executive agreement that the Attorney General has determined and certified to Congress satisfies a separate statutory provision (section 4). Subsection 3(a)(2) amends the Wiretap Act to establish that good faith reliance on such an order is a complete defense against any civil or criminal action.

Subsections 3(b)(1) and (2) similarly add additional exceptions to the SCA's general prohibition on accessing and disclosing stored communications and customer data (18 U.S.C. §§ 2702(b) and 2702(c), respectively) to respond to a foreign order pursuant to an executive agreement that meets the requirements of section 4. Subsection 3(b)(3) similarly amends the SCA to establish that good faith reliance on such an order is a complete defense against any civil or criminal action.

Subsection 3(c)(1) amends the Pen/Trap Statute to permit the installation of a pen register or a trap-and-trace device to respond to a foreign order pursuant to an executive agreement that meets the requirements of section 4. Subsections 3(c)(2) and 3(c)(3) amend the Pen/Trap Statute to bar criminal and civil causes of actions under the Pen/Trap Statute that stem from good-faith compliance with such a foreign order.

Section 4 creates a new section in Title 18 setting forth requirements for executive agreements such that foreign government orders covered by them would fall within the exceptions laid out in section 3. Subsection 4(a) establishes that an executive agreement will satisfy the statutory requirements of the new section if three conditions are met.

First, per subsection 4(a)(1), and taking into account, as appropriate, credible information and expert input, the Attorney General, with the concurrence of the Secretary of State, must determine and certify to Congress that the foreign government's domestic law, in light of the data collection and activities subject to the executive agreement, affords robust substantive and procedural protections for privacy and civil liberties, including by:

- (i) having adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated through accession to the Budapest Convention on Cybercrime, or through domestic laws that are consistent with definitions and the requirements set forth in Chapters I and II of that Convention;
- (ii) demonstrating respect for the rule of law and principles of non-discrimination;
- (iii) adhering to applicable international human rights obligations and commitments or demonstrating respect for international universal human rights (including but not limited to protection from arbitrary and unlawful interference with privacy; fair trial rights; freedoms of expression, association and peaceful assembly; prohibitions on arbitrary arrest and detention; and prohibitions against torture and cruel, inhuman, or degrading treatment or punishment);

- (iv) including clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective of oversight of these activities;
- (v) having sufficient mechanisms to provide accountability and appropriate transparency regarding the government's collection and use of electronic data; and
- (vi) demonstrating a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet.

Second, per subsection 4(a)(2), the Attorney General, with the concurrence of the Secretary of State, must determine and certify to Congress that the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of any information concerning U.S. persons obtained through the executive agreement. Specific procedures will be agreed upon and adopted as part of each executive agreement.

Third, per subsection 4(a)(3), the Attorney General, with the concurrence of the Secretary of State, must determine and certify to Congress that, with respect to orders issued pursuant to the executive agreement, the executive agreement requires that:

- (i) the foreign government may not intentionally target a U.S. person or person located in the United States, and must adopt targeting procedures to ensure such targeting does not occur;
- (ii) the foreign government 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;
- (iii) the foreign government may not issue an order at the request of or to obtain information to provide to the United States government or a third-party government, and the foreign government cannot be required to share information with the United States government or a third-party government;
- (iv) the foreign government orders must be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;
- (v) foreign government orders must target a specific person, account, address, or personal device or any other specific identifier (i.e., may not engage in bulk collection);

- (vi) foreign government orders must be issued in compliance with the foreign country's domestic law, and any obligation for a provider to produce data derives solely from that foreign government's law;
- (vii) foreign government orders must be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;
- (viii) foreign government orders must be subject to review or oversight by a court, judge, magistrate, or other independent authority;
- (ix) foreign government orders for the interception of wire or electronic communications, and any extensions thereof, must be for a fixed, limited duration; interception may last no longer than is reasonably necessary to accomplish the approved purposes of the order; and orders may only be issued where that same information could not reasonably be obtained by another less intrusive method;
- (x) foreign government orders may not be used to infringe freedom of speech;
- (xi) the foreign government must promptly review all material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those trained in applicable procedures;
- (xii) the foreign government must segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or seriously bodily harm to any person;
- (xiii) the foreign government may not disseminate the content of a communication of a U.S. person to U.S. authorities unless the communication (a) may be disseminated pursuant to Section 4(a)(3)(xii) and (b) relates to significant harm, or the threat thereof, to the United States or U.S. persons, including but not limited to crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud.
- (xiv) the foreign government must afford reciprocal rights of data access to the United States government;
- (xv) the foreign government must agree to periodic review of its compliance with the terms of the executive agreement by the U.S. government; and
- (xvi) the U.S. government must reserve the right to render the executive agreement inapplicable as to any order for which it concludes the executive agreement may not properly be invoked.

Subsection 4(b) provides that a determination or certification made under subsection 4(a) shall not be subject to judicial or administrative review.

Subsection 4(c) requires the Attorney General to give 60 days' notice to the Senate and House judiciary and foreign-affairs committees prior to making a subsection 4(a) determination or certification. The Attorney General must also publish any such determination or any termination of an executive agreement satisfying section 4 in the Federal Register as soon as is reasonably practicable.

Subsection 4(d) requires that the Attorney General, with the concurrence of the Secretary of State, renew a country's determination of eligibility for an executive agreement satisfying section 4 every five years. Absent such a renewal, the executive agreement will no longer satisfy Section 4.

Subsection 4(e) provides a definition of "United States person" for use in the new Title 18 section.

Section 5 establishes that nothing in the legislation precludes any foreign government from obtaining assistance in a criminal investigation or prosecution through other previously existing processes, such as mutual legal assistance requests.