JONES DAY | One Firm Worldwide®

WHITE PAPER

January 2020

Evidence Collection in Criminal Investigations: Cross-Border Issues and Corporate Employee Considerations

In this age of heightened international enforcement of corporate crime, it is critical that companies be prepared for the possibility that government authorities will employ a variety of investigative techniques to obtain evidence of suspected criminal activity. This preparation starts with developing a sound understanding of the ways in which government personnel may seek to obtain information from a company and its employees, and how the company and its employees may comply with or otherwise appropriately respond to such efforts.

This Jones Day *White Paper* highlights key methods by which the U.S. government may collect evidence from companies and their employees at the U.S. border and abroad, and outlines practical considerations for companies to bear in mind in anticipating and planning for the possibility of coming within the ambit of a criminal probe.

TABLE OF CONTENTS

INTRODUCTION

The U.S. government continues to set the pace in the investigation and enforcement of international corporate crime, but law enforcement authorities in other countries are gaining ground. Sometimes, U.S. law enforcement agencies act entirely on their own, without the involvement of counterparts from other countries; in other instances, U.S. agencies and foreign counterparts work in concert, coordinating investigative activities and sharing the fruits of those activities with one another. Particularly for multinational companies, the ever-increasing possibility that corporate conduct may have criminal and regulatory implications across multiple jurisdictions makes understanding government investigative practices all the more important.

FEDERAL AGENCY BORDER SEARCHES

The U.S. Department of Homeland Security ("DHS") has broad power to enforce federal law at the U.S. border.[1] Various federal statutes and regulations grant DHS—including two of its major operational components, the U.S. Customs and Border Protection ("CBP") and the U.S. Immigration and Customs Enforcement ("ICE")—the power to inspect and examine individuals and items entering or exiting the United States.[2] Border searches may also be conducted by officials from other U.S. agencies, including the Drug Enforcement Administration ("DEA") and the Federal Bureau of Investigation ("FBI").[3]

Constitutional Parameters of Border Searches

Although warrantless searches and seizures executed without probable cause typically violate the Fourth Amendment to the U.S. Constitution, the "border-search exception" to the warrant requirement allows warrantless searches of both U.S. citizens and non-citizens at an international border.[4] This border-search authority is premised in part on the reduced expectation of privacy associated with international travel.[5] As a practical matter, the border authority possessed by U.S. agencies means that corporate personnel—U.S. citizens and foreign nationals alike—are subject to government inspection simply by entering or leaving the United States.

Searches of international passengers at American airports are considered border searches because they occur at the "functional equivalent of a border."[6] Moreover, several federal appellate courts have adopted an "extended border search" doctrine, permitting U.S. government officials to conduct warrantless searches beyond the border or its functional equivalent, if certain criteria are met.[7] Courts have also held that the Fourth Amendment does not require a warrant for stops or searches of persons or property merely passing through the United States while in transit between two foreign countries.[8] Thus, all international travelers seeking to enter, depart, or pass through the United States should anticipate that U.S. officials could conduct warrantless searches of their persons and/or belongings.

In particular, the border-search exception allows U.S. government officials to detain, to inspect, and to examine all individuals entering or departing the U.S. Border searches are categorized as "routine" or "nonroutine" based on the level of intrusiveness, and the judicial scrutiny applied to searches varies based on this categorization. Routine border searches are not subject to any reasonable suspicion or probable cause requirement, and they may be conducted without a warrant.[9] Routine searches typically consist of document checks, pat-downs, or the emptying of pockets, and require no justification.[10] In a routine search, authorities may inspect cars, baggage, and goods entering the country, even if the traveler has only been absent from the country for a very brief period or is only entering the country briefly. During a routine search, the traveler may even be subjected to detention.[11] This detention may only be "a brief detention," and in the absence of facts justifying further detention, a traveler may not be further detained without giving consent.[12]

Conversely, "nonroutine" border searches are constitutionally permissible only if supported by reasonable suspicion, which is a "particularized and objective basis for suspecting the particular person stopped of criminal activity."[13] Nonroutine search procedures are those that may be intrusive, embarrassing, or destructive, including destructive searches of inanimate objects, prolonged detentions, strip searches, body cavity searches, and X-ray searches.[14]

Electronic Devices at the Border

It is often the case that international business travel gives rise to significant issues and risks from the standpoint of border searches and seizures. This is particularly true with respect to electronic devices. For the international business traveler, the portability of smart phones and other electronic devices

capable of housing huge amounts of electronic corporate data and the ability to access even larger caches of remotely stored data through devices and software can be as much a bane as a boon. While companies will go to great pains and expense to lock down their corporate data—often their most valuable asset—as a protection against intrusion and theft by inside and outside elements, a single employee traveling internationally can expose that same data to immediate review and seizure by authorities at the border who will almost certainly not share the employee's understanding of, or concern for, the data's sensitivity.

Border searches of electronic devices, such as laptop computers, tablets, and mobile phones, present a unique set of practical and legal challenges. These searches can be particularly intrusive, given that electronic devices often contain vast amounts of confidential and sensitive information. Still, most courts that have considered the issue have found that a manual search of an electronic device is "routine," and that a warrantless and suspicionless search of such a device is reasonable under the Fourth Amendment.[15] Furthermore, if the government authorities involved have reasonable suspicion that a device contains evidence of a crime, they are authorized to review (and even electronically copy) data from the device without a warrant.[16]

However, recent court decisions have challenged the majority position that border searches of electronic devices are routine. In *Alasaad v. Nielsen*, a United States District Court judge in the District of Massachusetts held that both "basic" and "advanced"[17] searches of electronic devices are indeed *non-routine* searches.[18] The *Alasaad* court reasoned that "electronic devices carried by travelers, including smartphones and laptops, can contain a very large volume of information, including 'sensitive information,'"[19] and, accordingly, concluded that "agents and officials must have reasonable suspicion to conduct any search of entrants' electronic devices."[20] The court also emphasized that "[t]his requirement reflects both the important privacy interests involved in searching electronic devices and the Defendant's governmental interests at the border."[21]

Further, in *United States v. Aigbekaen,* the United States Court of Appeals for the Fourth Circuit—describing searches of electronic devices as "intrusive and nonroutine"[22]— recently held that, in order to conduct a warrantless search of a traveler's electronic devices at the border, "the Government must have individualized suspicion of an offense that bears some nexus to the border search exception's purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband."[23] It remains to be seen whether the rule relating to suspicionless border searches, as set forth in *Alasaad* and *Aigbekaen*, will be adopted by other courts.

As noted in the *Alasaad* opinion, CBP and ICE have both issued policies regarding the search and inspection of electronic devices at the international border by their respective personnel.[24] Though the policies appear similar in nature, ICE's policy allows for more prolonged investigations—searches conducted under CBP's policy are not to exceed five days,[25] whereas ICE's policy provides that searches should generally be finished within 30 days of the date of detention, unless circumstances warrant extra time.[26] If CBP turns a device over to ICE for analysis and investigation, ICE policy applies once the device is received by ICE.[27]

It should be noted that under these policies, a search of an electronic device's contents may only include an examination of the information on the device itself that is accessible through the device's operating system or through other software, tools, or applications.[28] As such, officers may not intentionally use a device to access information stored remotely.[29] Prior to the search of a device, a traveler may disable connectivity to any network (e.g., by placing the device in "airplane mode") or request that the searching officer do so.[30]

In addition, officers may not make changes to the contents of a device during the course of a border search.[31] To gain access to a passcode-protected or encrypted device, officers may request a passcode or other means of access from an individual, but any passcode given must be deleted or destroyed by the agency following the search of that device.[32] And, if a traveler does not provide a passcode, officers may detain the device pending a determination as to its admissibility, exclusion, or other disposition, and may "seek technical advice, use external equipment, pursue legal remedies, or take other reasonable measures" to inspect the device.[33] If probable cause arises from the border search of a device, CBP and ICE officers are authorized under their agency policies to seize the device or copy the information from the device.[34] Absent probable cause, officers may only retain information relating to immigration, customs, and other enforcement matters.[35]

While these policies were written against the legal framework established by courts holding that suspicionless searches of electronic devices are reasonable under the Fourth Amendment, it is plausible that these policies could be subject to revision, particularly if the *Alasaad* and *Aigbekaen* holdings evolve into the majority position. In the meantime, international travelers would be well served by accounting for the possibility that, whether premised on individualized suspicion or not, their electronic devices may be inspected by border officials and that an inspection may, in turn, result in the review and electronic copying of the contents of those devices without a warrant. With this broad authority in mind, and to avoid the inconvenience and disruption that such a search would inevitably entail, employees traveling across the U.S. border should consider bringing with them only the data or documents that are necessary to any business the employees intend to conduct while away or avoiding the physical transport of data or documents altogether and instead accessing the same through remote means once the employees have arrived at their destination. And, of course, if subject to a border search, corporate personnel should comply with CPB and ICE directives, subject to their constitutional protections and the scope of the applicable regulations.

Considerations for Corporate Counsel

If corporate counsel is stopped at the border and searched, counsel should identify any seized documents or data that are protected by the attorney-client privilege or the attorney work-product doctrine.[36] Any privileged information should then be separated from other information via a CBP "Filter Team" comprised of legal and operational representatives.[37] Agency policy provides that, following CBP's review, materials determined to be privileged will be destroyed, except for materials maintained "in coordination with the CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law."[38] Any business or commercial information encountered by CBP officers during a search must be treated as confidential business information and be protected from unauthorized disclosure.[39]

Given the impact of an appropriate privilege assertion, corporate counsel entering or leaving the United States should anticipate the possibility of being stopped and searched at the border, and should be prepared to identify qualifying materials in counsel's possession as privileged and, if necessary, to seek to ensure that the "Filter Team" review process described above is employed.

Questioning by the U.S. Government at the Border

In addition to conducting searches and seizures, the U.S. government has the ability to question individuals at the border. A person seeking entry into the United States typically does not have a right to remain silent and is not entitled to the aid of legal counsel[40] at the primary or secondary inspection stage, so long as any questioning pertains to the customs or immigration process.[41] A traveler must first be removed from the routine processes of border questioning and questioned or searched individually before *Miranda* rights are triggered.[42] And, questioning must go beyond the scope of the routine customs process before the rights to counsel and to silence apply.[43] These rights attach only when "questioning at the border [rises] to a distinctly accusatory level [and] it can be said that a reasonable person would feel restraints on his ability to roam to the degree associated with formal arrest."[44] Thus, if confronted with questioning at the border that shifts from issues related to admission into the United States to instead focus on potential corporate criminal activity, the international business traveler enjoys, and may properly consider invoking, the constitutional right to counsel and the right to remain silent.

OBTAINING EVIDENCE THROUGH CORPORATE EMPLOYEES OUTSIDE THE UNITED STATES

Additional considerations arise from the U.S. government's power to collect evidence abroad. The methods by which the government may do so, along with the limitations on this authority and related considerations for companies and corporate employees, are outlined below.

Serving a Subpoena on a Corporate Employee Outside the United States

Under certain circumstances, a subpoena can be properly issued and served on corporate employees located outside the United States [45] In particular, 28 U.S.C. § 1783 authorizes a U.S. court to issue a subpoena requiring a U.S. citizen or permanent resident located in a foreign country to either appear as a witness or produce a specified document or other record.[46] In order to do so, the court must find that the testimony or production of the document or other record is necessary in

the interest of justice.[47] Additionally, the court must conclude that the testimony cannot be obtained without the witness's personal appearance or that the production of the document or other record cannot be obtained in any other way.[48] The subpoena should state the time and place for appearance or for the production of the document or other record.[49]

If the subpoena is served but the recipient fails to appear or to produce requested documentation, 28 U.S.C. § 1784 authorizes a U.S. court to order the served person to show cause.[50] The court may also order that property in the United States belonging to the served person be seized to satisfy any judgment, should the person be found in contempt for the failure to appear or produce requested documents or records.[51] If the served person is found to be in contempt of court, the court may issue a fine that should not exceed $100,000.[52] The seized property may also be sold to satisfy fines and costs associated with the judgment.[53]

Courts have held that Section 1783 does not apply to foreign nationals residing outside the United States,[54] and there is no U.S. statute that authorizes the issuance and service of a subpoena on a non-U.S. citizen or resident who is not physically present in the United States. As such, a U.S. court cannot issue a subpoena to a foreign national residing in a foreign country.[55] Indeed, "[t]he government has no power to compel the presence of a foreign national residing outside the United States."[56]

Section 702 Surveillance

Under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), however, the U.S. government may collect evidence through, among other things, electronic surveillance of communications involving non-U.S. citizens living abroad.[57] Under FISA, the communications to be surveilled must be facilitated by U.S.-based electronic communications service providers, and obtaining foreign intelligence information must be a significant purpose of the surveillance.[58] A separate court order is not necessary to conduct surveillance of a particular individual pursuant to FISA Section 702.[59] Instead, annual certifications submitted by the U.S. Attorney General and the U.S. Director of National Intelligence defining the categories of individuals who may be appropriately targeted provide the basis for the surveillance.

Corporate personnel should be aware that the collection of evidence from non-U.S. citizens in foreign countries pursuant to Section 702 can lead to the incidental collection of communications of U.S. citizens. In this regard, the general rule is that "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."[60]

MLAT Process

While aside from the FISA process, the U.S. government is restricted from gathering evidence outside the United States from non-U.S. citizens, the United States has entered into Mutual Legal Assistance Treaties ("MLATs") with certain foreign countries to help facilitate legal proceedings and mutual assistance in criminal matters. The basic purpose of an MLAT is to provide "bilateral, mutual assistance in the gathering of legal evidence for use by the requesting state in criminal investigations and proceedings."[61] The United States has MLATs with a number of foreign countries, including Canada, the Netherlands, Switzerland, and Russia.[62]

MLATs are self-executing treaties—that is, they take effect immediately upon ratification and do not require Congress to enact any law for the treaty to have force within the United States [63] When an MLAT is established between the United States and another country, it is generally understood that the governments of the respective countries will assist one another in criminal investigations by, among other actions, serving documents; taking testimony or other statements from individuals; and providing documents, records, or other materials in response to a request.

While MLAT requests can thus lead to the acquisition of relevant information in many U.S. government investigations from non-U.S. citizens, MLATs are typically not a favored approach of investigating officials. This is because, among other things, the MLAT process is time-consuming and, of course, necessarily relies heavily upon the cooperation of the recipient authority.

The subject of an information request under an MLAT has no right of participation in the process, nor is the subject provided notice of the U.S. government's MLAT request to another country. Most often, the subject of the MLAT request only finds out about the request as a result of a criminal prosecution relating to the request. Further, courts have consistently held that MLATs do not create private rights, and the terms of most MLATs do not give subjects the right to exclude evidence or to impede the execution of an MLAT request.[64]

PREPARING EMPLOYEES FOR POSSIBLE GOVERNMENT CONTACT

Keeping in mind the myriad ways in which U.S. officials can seek information from corporate employees, companies can help their employees by appropriately informing them of their rights and of what the U.S. government can and cannot compel them to do. Specifically, the following topics may be useful to address with employees so that they are prepared for the possibility that they may be searched, detained, interviewed, and/or subpoenaed by U.S. law enforcement authorities and knowledgeable about their rights and appropriate conduct in the context of interactions with such authorities:

- The ways in which the government may try to contact them;
- The possibility of a search, questioning, and detention at the border;
- Their right to speak to a lawyer before answering questions from a government official that extend beyond matters related to their admission into the United States;
- The circumstances under which they have a right to remain silent in response to government questioning;
- Their right to speak with the government if they choose to do so;
- Best practices for traveling with electronics, including with respect to safeguarding proprietary and confidential business information and attorney-client privileged materials;
- The importance of avoiding conduct that could serve as the basis for a claim that they obstructed justice;
- A company request that they report to the company any contacts with the government or subpoenas received in connection with their employment; and
- Tactics and requests by the government that likely fall outside the scope of what a U.S. official can lawfully ask an employee to do.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

AUTHORS

Theodore T. Chung
Chicago
+1.312.269.4234
ttchung@jonesday.com

Bethany K. Biesenthal
Chicago
+1.312.269.4303
bbiesenthal@jonesday.com

Leigh A. Krahenbuhl
Chicago
+1.312.269.1524
lkrahenbuhl@jonesday.com

Jules H. Cantor
Chicago
+1.312.269.1503
jcantor@jonesday.com

Associate Katelyn E. Nicasio assisted in the preparation of this White Paper.

ADDITIONAL LAWYER CONTACTS

Richard H. Deane, Jr.
Atlanta
+1.404.581.8502
rhdeane@jonesday.com

Ryan M. Disantis
Boston
+1.617.449.6911
rdisantis@jonesday.com

James C. Dunlop
Chicago / São Paulo
+1.312.269.4069 / +55.11.3018.3939
jcdunlop@jonesday.com

Louis P. Gabel
Detroit
+1.313.230.7955
lpgabel@jonesday.com

Jamila M. Hall
Atlanta
+1.404.581.8465
jhall@jonesday.com

Karen P. Hewitt
San Diego
+1.858.314.1119
kphewitt@jonesday.com

Adam Hollingsworth
Cleveland
+1.216.586.7235
ahollingsworth@jonesday.com

Samir C. Jain
Washington
+1.202.879.3848
sjain@jonesday.com

James T. Kitchen
Pittsburgh
+1.412.394.7272
jkitchen@jonesday.com

James P. Loonam
New York
+1.212.326.3808
jloonam@jonesday.com

Andrew M. Luger
Minneapolis
+1.612.217.8862
aluger@jonesday.com

Shireen Matthews
San Diego
+1.858.314.1184
shireenmatthews@jonesday.com

Christopher R.J. Pace
Miami
+1.305.714.9730
crjpace@jonesday.com

Christopher K. Pelham
Shanghai / Los Angeles
+86.21.2201.8000 / +1.213.243.2686
cpelham@jonesday.com

Cristina Pérez Soto
Miami
+1.305.714.9733
cperezsoto@jonesday.com

Mary Ellen Powers
Washington
+1.202.879.3870
mepowers@jonesday.com

Peter J. Romatowski
Washington
+1.202.879.7625
pjromatowski@jonesday.com

Ronald W. Sharpe
Washington
+1.202.879.3618
rsharpe@jonesday.com

Rasha Gerges Shields
Los Angeles
+1.213.243.2719
rgergesshields@jonesday.com

Shamoil T. Shipchandler
Dallas / Houston
+1.214.969.3684 / +1.832.239.3753
sshipchandler@jonesday.com

Eric Snyder
São Paulo / New York
+55.11.3018.3925 /+1.212.326.3435
esnyder@jonesday.com

Stephen G. Sozio
Cleveland
+1.216.586.7201
sgsozio@jonesday.com

Neal J. Stephens
Silicon Valley
+1.650.687.4135
nstephens@jonesday.com

Brian A. Sun
Los Angeles
+1.213.243.2858
basun@jonesday.com

Edward Patrick Swan, Jr.
San Diego
+1.858.703.3132
pswan@jonesday.com

Jason S. Varnado
Houston
+1.832.239.3694
jvarnado@jonesday.com

Hank Bond Walther
Washington
+1.202.879.3432
hwalther@jonesday.com

James R. Wooley
Cleveland
+1.216.586.7345
jrwooley@jonesday.com

ENDNOTES

1 *See* 6 U.S.C. § 202 (2018) (defining DHS responsibilities).

2 *See, e.g.*, 8 U.S.C. §, 1357 (2018); 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1595a (2018); 22 C.F.R. § 127.4 (2019); 19 C.F.R. § 162.6 (2019) ("All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer.").

3 *United States v. Levy*, 803 F.3d 120, 124 (2d Cir. 2015) (discussing the DEA and FBI, and concluding: "We see no constitutional reason to prevent these and other federal law enforcement agents from also supplying information to Customs officials in aid of a border search."); *see also* 8 C.F.R. § 287.5 (2019) (listing officers authorized and designated to exercise the power to patrol the border).

4 *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (citation omitted) ("[S]earches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.").

5 *Id.* at 154 (noting that "the expectation of privacy is less at the border than it is in the interior").

6 *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973) ("[A] search of the passengers and cargo of an airplane arriving at a St. Louis airport after a non-stop flight from Mexico City would clearly be the functional equivalent of a border search.").

7 *Investigations and Police Practices*, 47 GEO. L.J. ANN. REV. CRIM. PROC. 3, 156 (2018) (explaining that there must be 1) "reasonable certainty" or a "high degree of probability" that a border was crossed; 2) "reasonable certainty" that no change in the object of the search has occurred between the time of crossing and the search; and 3) "reasonable suspicion" that criminal activity is occurring).

8 *United States v. Garcia*, 905 F.2d 557, 559 (1st Cir. 1990).

9 *Bryan v. United States*, 913 F.3d 356, 361 (3d Cir. 2019) (comparing routine and nonroutine searches).

10 *See United States v. Saboonchi*, 990 F. Supp. 2d 536, 549 (D. Md. 2014) (collecting cases).

11 *United States v. Nava*, 363 F.3d 942, 945 (9th Cir. 2004).

12 United States v. Ludlow, 992 F.2d 260, 264-65 (10th Cir. 1993) (initial detention pursuant to routine stop lasted only 45 seconds; further facts gave rise to suspicion warranting further detention).

13 *United States v. Cortez*, 449 U.S. 411, 417-18 (1981).

14 *See United States v. Saboonchi*, 990 F. Supp. 2d 536, 550-51 (D. Md. 2014) (collecting cases).

15 *United States v. Cotterman*, 709 F.3d 952, 967 (9th Cir. 2013).

16 Border Search of Electronic Devices, CBP Directive No. 3340-049A, § 5.5.1 (Jan. 4, 2018).

17 "Under [both CPB and ICE policy], an advanced search is defined as 'any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to the device, but to review, copy and/or analyze its contents,'" while "[a] basic search is defined as 'any border search that is not an advanced search.'" *Alasaad v. Nielsen*, 2019 WL 5899371, at *2 (D. Mass. Nov. 12, 2019).

18 *Id.* at *14.

19 *Id.* at *13.

20 *Id.* at *14.

21 *Id.*

22 *United States v. Aigbekaen*, 2019 WL 6200236, at *4 (4th Cir. Nov. 21, 2019).

23 *Id.*

24 Border Searches of Electronic Devices, ICE Directive No 7-6.1 (Aug. 18, 2009); Border Search of Electronic Devices Containing Information, CBP Directive No. 3340-049 (Aug. 20, 2009).

25 Border Search of Electronic Devices, CBP Directive No. 3340-049A, § 5.4.1 (Jan. 4, 2018).

26 Border Searches of Electronic Devices, ICE Directive No 7-6.1, § 8.3 (Aug. 18, 2009).

27 *Id.* § 6.2.

28 Border Search of Electronic Devices, CBP Directive No. 3340-049A, § 5.1.2 (Jan. 4, 2018).

29 *Id.*

30 *Id.*

31 *Id.*

32 *Id.* at § 5.3.2.

33 *Id.* at §§ 5.3.3, 5.3.4.

34 Border Searches of Electronic Devices, ICE Directive No 7-6.1, § 8.5(a) (Aug. 18, 2009); Border Search of Electronic Devices, Border Search of Electronic Devices, CBP Directive No. 3340-049A, § 5.5.1.1 (Jan. 4, 2018).

35 Border Searches of Electronic Devices, ICE Directive No 7-6.1, § 8.5(b) (Aug. 18, 2009); Border Search of Electronic Devices, CBP Directive No. 3340-049A, § 5.5.1.2 (Jan. 4, 2018).

36 *Id.* at § 5.2.1.1.

37 *Id.* at § 5.2.1.2.

38 *Id.* at § 5.2.1.3.

39 *Id.* at § 5.2.3.

40 *United States v. Gupta*, 183 F.3d 615, 617 (7th Cir. 1999).

41 8 C.F.R. § 292.5(b).

42 *United States v. Beras*, 918 F. Supp. 38 (D.P.R. 1996).

43 *United States v. Ventura*, 947 F. Supp. 25, 29 (D.P.R. 1996) (*remanded on other grounds* by routine *United States v. Fernandez-Ventura*, 132 F.3d 844, 848 (1st Cir. 1998)).

44 *U.S. v. Moya*, 74 F.3d 1117, 1120 (11th Cir. 1996) (internal quotations omitted).

45 While means by which U.S. law enforcement authorities may seek to compel the production of, or otherwise obtain, information from persons and other sources outside the U.S. through formal process are addressed below, It should be noted that persons residing outside the U.S. may agree to provide information to U.S. law enforcement authorities on a purely voluntary basis.

46 28 U.S.C. § 1783(a).

47 *Id.*

48 *Id.*

49 28 U.S.C. § 1783(b).

50 28 U.S.C. § 1784(a).

51 28 U.S.C. § 1784(b).

52 28 U.S.C. § 1784(d).

53 *Id.*

54 *See United States v. Gordon*, 634 F.2d 639, 645-46 (1st Cir. 1980).

55 *See United States v. Haim*, 218 F. Supp. 922, 926 (S.D.N.Y. 1963).

56 *United States v. Theresius Filippi*, 918 F.2d 244, 247 (1st Cir. 1990).

57 50 U.S.C. § 1881a(a).

58 50 U.S.C. § 1881a(h)(2)(v-vi).

59 *See U.S. v. Mohamud*, 2014 WL 2866749, at *27 (D. Or. June 24, 2014).

60 *Id.*

61 *In re Req. from United Kingdom Pursuant to Treaty Between Govt. of U.S. and Govt. of United Kingdom on Mut. Assistance in Crim. Matters in the Matter of Dolours Price*, 685 F.3d 1, 9 (1st Cir. 2012).

62 *In re Premises Located at 840 140th Ave. NE, Bellevue, Wash*., 634 F.3d 557, 564 (9th Cir. 2011).

63 *Id.* at 568.

64 *In re Request from United Kingdom,* 685 F.3d at 12; *United States v. Chitron Electronics Co. Ltd.*, 668 F. Supp. 2d 298, 306-07 (D. Mass. 2009).