Knight First Amend. Inst. at Columbia Univ. v. Dep't of Homeland Sec.
No. 1:17-cv-00548-TSC

Answer

Ex. A

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049 DATE: August 20, 2009

ORIGINATING OFFICE: FO:TO

SUPERSEDES:

REVIEW DATE: August 2012

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION

1 PURPOSE. To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices, encountered by U.S. Customs and Border Protection (CBP) at the border, both inbound and outbound, to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce.

These searches are part of CBP's long-standing practice and are essential to enforcing the law at the U.S. border. Searches of electronic devices help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations. Finally, searches at the border are often integral to a determination of admissibility under the immigration laws.

2 POLICY.

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air Interdiction Agents, Marine Interdiction Agents, and other employees authorized by law to perform searches at the border, the functional equivalent of the border (FEB), or the extended border shall adhere to the policy described in this Directive.

2.3 This Directive governs border search authority only. It does not limit CBP's authority to conduct other lawful searches at the border, e.g., pursuant to a warrant, consent, or incident to an arrest; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., a shipment of hundreds of laptop computers transiting from the factory to the distributor).

2.5 This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede *Processing Foreign Diplomatic and Consular Officials*, Directive 3340-032. Diplomatic and consular officials encountered at the border, the FEB, or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), ICE Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.

3 DEFINITIONS.

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air Interdiction Agent, Marine Interdiction Agent, Internal Affairs Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. Includes any devices that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices.

3.3 Destruction. For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

3.4 Border Search of Information. Excludes actions taken to determine if a device functions (e.g., turning an electronic device on and off), or actions taken to determine if contraband is concealed within the device itself. The definition also excludes the review of information voluntarily provided by an individual in an electronic format (for example, when an individual voluntarily shows an e-ticket on an electronic device to an Officer).

4 AUTHORITY/REFERENCES. 8 U.S.C. 1225, 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051), Directive 5240-005.

5 PROCEDURES.

5.1 Border Searches.

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. 507).

5.1.2 In the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.3 Searches of electronic devices will be documented in appropriate CBP systems of records and should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire search, or where a supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.4 Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material.

5.2.1 Officers may encounter materials that appear to be legal in nature, or an individual may assert that certain information is protected by attorney-client or attorney work product privilege. Legal materials are not necessarily exempt from a border search, but they may be subject to the following special handling procedures: If an Officer suspects that the content of such a material may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the Officer must seek advice from the CBP Associate/Assistant Chief Counsel before conducting a search of the material, and this consultation shall be noted in appropriate CBP systems of records. CBP counsel will coordinate with the U.S. Attorney's Office as appropriate.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel, and this consultation shall be noted in appropriate CBP systems of records.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with federal agencies that have mechanisms in place to protect appropriately such information.

5.3 Detention and Review in Continuation of Border Search of Information

5.3.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days.

5.3.1.1 Approval of and Time Frames for Detention. Supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director, Patrol Agent in Charge, or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems of records.

5.3.1.2 Destruction. Except as noted in section 5.4 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.3, there is not probable cause to seize it, any copies of the information must be destroyed, and any electronic device must be returned. Upon this determination that there is no value to the information copied from the device, the copy of the information is destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system of records and which must be no later than twenty one (21) days after such determination. The destruction shall be noted in appropriate CBP systems of records.

5.3.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, and when the fact of conducting this search can be disclosed to the individual transporting the device without hampering national security or

law enforcement or other operational considerations, the individual may be notified of the purpose and authority for these types of searches, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search.

5.3.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.3.2 Assistance by Other Federal Agencies.

5.3.2.1 The use of other federal agency analytical resources outside of CBP and ICE, such as translation, decryption, and subject matter expertise, may be needed to assist CBP in reviewing the information contained in electronic devices or to determine the meaning, context, or value of information contained in electronic devices.

5.3.2.2 Technical Assistance – With or Without Reasonable Suspicion. Officers may sometimes have technical difficulties in conducting the search of electronic devices such that technical assistance is needed to continue the border search. Also, in some cases Officers may encounter information in electronic devices that requires technical assistance to determine the meaning of such information, such as, for example, information that is in a foreign language and/or encrypted (including information that is password protected or otherwise not readily reviewable). In such situations, Officers may transmit electronic devices or copies of information contained therein to seek technical assistance from other federal agencies. Officers may seek such assistance with or without individualized suspicion.

5.3.2.3 Subject Matter Assistance by Other Federal Agencies – With Reasonable Suspicion. In addition to encountering information in electronic devices that is in a foreign language, encrypted, or requires technical assistance, Officers may encounter information that requires referral to subject matter experts in other federal agencies to determine the meaning, context, or value of information contained therein as it relates to the laws enforced and administered by CBP. Therefore, Officers may transmit electronic devices or copies of information contained therein to other federal agencies for the purpose of obtaining subject matter assistance when they have reasonable suspicion of activities in violation of the laws enforced by CBP. While many factors may result in reasonable suspicion, the presence of an individual on a government-operated and government-vetted terrorist watch list will be sufficient to create reasonable suspicion of activities in violation of the laws enforced by CBP.

5.3.2.4 Approvals for seeking translation, decryption, and subject matter assistance. Requests for translation, decryption, and subject matter assistance require supervisory approval and shall be properly documented and recorded in CBP systems of records. If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual

prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.3.2.5 Electronic devices should be transmitted only when necessary to render the requested translation, decryption, or subject matter assistance. Otherwise, a copy of such information should be transmitted in lieu of the device in accord with this Directive.

5.3.2.6 When information from an electronic device is transmitted to another federal agency for translation, decryption, or subject matter assistance, the individual will be notified of this transmission unless CBP determines, in consultation with the receiving agency or other agency as appropriate, that notification would be contrary to national security or law enforcement or other operational interests. If CBP's transmittal seeks assistance regarding possible terrorism, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the transmittal or his or her presence on a watch list. When notification is made to the individual, the Officer will annotate the notification in CBP systems of records and on the Form 6051D.

5.3.3 Responses and Time for Assistance

5.3.3.1 Responses Required. Agencies receiving a request for assistance in conducting a border search are to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced by CBP.

5.3.3.2 Time for Assistance. Responses from assisting agencies are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager, responses from an assisting agency should be received within fifteen (15) days. If the assisting agency is unable to respond in that period of time, the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager may permit extensions in increments of seven (7) days.

5.3.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance being provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency to return to CBP all electronic devices that had been provided to the assisting agency, and any copies thereof, as expeditiously as possible, except as noted in 5.4.2.3. Any such revocation shall be documented in appropriate CBP systems of records. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency pursuant to the procedures outlined in this Directive.

5.3.3.4 Destruction. Except as noted in section 5.4.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the information does not exist, CBP will retain no copies of the information.

5.4 Retention and Sharing of Information Found in Border Searches

5.4.1 Retention and Sharing of Information Found in Border Searches

5.4.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents thereof, contains evidence of or is the fruit of a crime that CBP is authorized to enforce.

5.4.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. For example, information collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or ENFORCE or other systems as may be appropriate and consistent with the policies governing such systems.

5.4.1.3 Sharing Generally. Nothing in this Directive limits the authority of CBP to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.

5.4.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is mandated by statute, Presidential Directive, or DHS policy. Consistent with 6 U.S.C. 122(d)(2) and other applicable law and policy, CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with elements of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the element receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.4.1.5 Safeguarding Data During Storage and Transmission. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during transmission to another federal agency. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during transmission such as password

protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the Port Director, Patrol Agent in Charge or equivalent level manager and the CBP Office of Internal Affairs.

5.4.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.4.2 Retention by Agencies Providing Translation, Decryption, or Subject Matter Assistance

5.4.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting federal agency may be retained by that agency for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.4.2.3 below.

5.4.2.2 Return or Destruction. At the conclusion of the requested assistance, all information must be returned to CBP as expeditiously as possible, and the assisting agency must advise CBP in accordance with section 5.3.3 above. In addition, the assisting federal agency should destroy all copies of the information transferred to that agency unless section 5.4.2.3 below applies. In the event that any electronic devices are transmitted, they must not be destroyed; they are to be returned to CBP unless seized by the assisting agency based on probable cause or retained per 5.4.2.3.

5.4.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency shall assume responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency only if and to the extent that it has the independent legal authority to do so—for example, when the information relates to terrorism or national security and the assisting agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.5 Reporting Requirements

5.5.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

5.5.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.3.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.5.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.6 Management Requirements

5.6.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.6.2 The appropriate CBP Second line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.6.3 The appropriate CBP Second line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another federal agency.

5.6.4 The Director, Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of information contained therein in order to ensure compliance with the procedures outlined in this Directive.

6 MEASUREMENT. CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.

7 AUDIT. CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 NO PRIVATE RIGHT CREATED. This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 DISCLOSURE. This Directive may be shared with the public.

10. SUPERSEDES. Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008) to the extent they pertain to electronic devices.

Acting Commissioner
U.S. Customs and Border Protection