

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

Answer

Ex. B

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT**  
**ICE Policy System**

**DISTRIBUTION:** ICE  
**DIRECTIVE NO.:** 7-6.1  
**ISSUE DATE:** August 18, 2009  
**EFFECTIVE DATE:** August 18, 2009  
**REVIEW DATE:** August 18, 2012  
**SUPERSEDES:** See Section 3 Below.

**DIRECTIVE TITLE: BORDER SEARCHES OF ELECTRONIC DEVICES**

**1. PURPOSE and SCOPE.**

- 1.1.** This Directive provides legal guidance and establishes policy and procedures within U.S. Immigration and Customs Enforcement (ICE) with regard to border search authority to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border, the functional equivalent of the border, and the extended border to ensure compliance with customs, immigration, and other laws enforced by ICE. This Directive applies to searches of electronic devices of all persons arriving in, departing from, or transiting through the United States, unless specified otherwise.
- 1.2.** This Directive applies to border search authority only. Nothing in this Directive limits the authority of ICE Special Agents to act pursuant to other authorities such as a warrant, a search incident to arrest, or a routine inspection of an applicant for admission.

- 2. AUTHORITIES/REFERENCES.** 8 U.S.C. § 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 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; and the December 12, 2008, ICE Office of Investigations (OI) guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices."

- 3. SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES.** ICE Directive No. 7-6.0 entitled "Border Searches of Documents and Electronic Media" is hereby superseded as it relates to electronic devices. Additionally, all other issuances on this subject issued by ICE prior to the date of this Directive are hereby superseded as they relate to searches of electronic devices, with the exception of the March 5, 2007, OI guidance entitled "Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry" and the December 12, 2008, OI guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media."

4. **BACKGROUND.** ICE is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, Special Agents may review and analyze computers, disks, hard drives, and other electronic or digital storage devices. These searches are part of ICE's long-standing practice and are essential to enforcing the law at the United States border. Searches of electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography; laundering monetary instruments; violations of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.
5. **DEFINITIONS.** The following definitions are provided for the purposes of this Directive:
  - 5.1. **Assistance.** The use of third party analytic resources such as language processing, decryption, and subject matter expertise, to assist ICE in viewing the information contained in electronic devices or in determining the meaning, context, or value of information contained therein.
  - 5.2. **Electronic Devices.** Any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices.
6. **POLICY.**
  - 6.1. ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the guidelines and applicable laws set forth herein. Assistance to complete a border search may be sought from other Federal agencies and non-Federal entities, on a case by case basis, as appropriate.
  - 6.2. When U.S. Customs and Border Protection (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.
  - 6.3. Nothing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems.
7. **RESPONSIBILITIES.**
  - 7.1. The Directors of OI, the Office of Professional Responsibility (OPR), and the Office of International Affairs (OIA) have oversight over the implementation of the provisions of this Directive.
  - 7.2. Special Agents in Charge (SACs) and Attachés are responsible for:

- 1) Implementing the provisions of this Directive and ensuring that Special Agents in their area of responsibility (AOR) receive a copy of this Directive and are familiar with its contents;
- 2) Ensuring that Special Agents in their AOR have completed any training programs relevant to border searches of electronic devices, including constitutional, privacy, civil rights, and civil liberties training related to such searches, as may be required by ICE Headquarters; and
- 3) Maintaining appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this Directive. (See "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices" memo dated December 12, 2008.)

**7.3.** Attachés are responsible for ensuring coordination with their host countries, as appropriate, before conducting any such border search outside of the United States.

**7.4.** When ICE receives electronic devices, or copies of information therefrom, from CBP for analysis and investigation, ICE Special Agents are responsible for advising CBP of the status of any such analysis within 10 calendar days, and periodically thereafter, so that CBP records may be updated as appropriate. For example, "search ongoing"; "completed with negative results"; "returned to traveler"; or "seized as evidence of a crime."

**7.5.** Special Agents are responsible for complying with the provisions of this Directive, knowing the limits of ICE authority, using this authority judiciously, and ensuring comprehension and completion of any training programs relevant to border searches of electronic devices as may be required by ICE.

## **8. PROCEDURES.**

### **8.1. Border Searches by ICE Special Agents.**

- 1) Authorization to Conduct Border Search. Border searches of electronic devices must be performed by an ICE Special Agent who meets the definition of "customs officer" under 19 U.S.C. § 1401(i), or another properly authorized officer with border search authority, such as a CBP Officer or Border Patrol Agent, persons cross designated by ICE as customs officers, and persons whose assistance to ICE is demanded under 19 U.S.C. § 507.
- 2) Knowledge and Presence of the Traveler. To the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler. When not practicable due to law enforcement, national security, or other operational concerns, such circumstances are to be noted by the Special Agent in appropriate ICE systems. 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 concerns, the individual will not be permitted to observe the search.

- 3) Consent Not Needed. At no point during a border search of electronic devices is it necessary to ask the traveler for consent to search.
- 4) Continuation of the Border Search. At any point during a border search, electronic devices, or copies of information therefrom, may be detained for further review either on-site at the place of detention or at an off-site location, including a location associated with a demand for assistance from an outside agency or entity (see Section 8.4).
- 5) Originals. In the event electronic devices are detained, the Special Agent should consider whether it is appropriate to copy the information therefrom and return the device. When appropriate, given the facts and circumstances of the matter, any such device should be returned to the traveler as soon as practicable. Consultation with the Office of the Chief Counsel is recommended when determining whether to retain a device in an administrative immigration proceeding. Devices will be returned to the traveler as expeditiously as possible at the conclusion of a negative border search.

## **8.2. Chain of Custody.**

- 1) Detentions of electronic devices. Whenever ICE detains electronic devices, or copies of information therefrom, the Special Agent will initiate the correct chain of custody form or other appropriate documentation.
- 2) Seizures of electronic devices for criminal purposes. Whenever ICE seizes electronic devices, or copies of information therefrom, the Special Agent is to enter the seizure into the appropriate ICE systems. Additionally, the seizing agent must complete the correct chain of custody form or other appropriate documentation.
- 3) Retention of electronic devices for administrative immigration purposes. Whenever ICE retains electronic devices, or copies of information therefrom, or portions thereof, for administrative immigration purposes pursuant to 8 U.S.C. § 1357, the Special Agent is to record such retention in appropriate ICE systems and is to include the location of the retained files, a summary thereof, and the purpose for retention.
- 4) Notice to traveler. Whenever ICE detains, seizes, or retains original electronic devices, the Special Agent is to provide the traveler with a copy of the applicable chain of custody form or other appropriate documentation.

## **8.3. Duration of Border Search.**

- 1) Special Agents are to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search. Searches are generally to be completed within 30 calendar days of

the date of detention, unless circumstances exist that warrant more time. Such circumstances must be documented in the appropriate ICE systems. Any detention exceeding 30 calendar days must be approved by a Group Supervisor or equivalent, and approved again every 15 calendar days thereafter, and the specific justification for additional time documented in the appropriate ICE systems.

- 2) Special Agents seeking assistance from other Federal agencies or non-Federal entities are responsible for ensuring that the results of the assistance are received in a reasonable time (see Section 8.4(5)).
- 3) In determining “reasonable time,” courts have reviewed the elapsed time between the detention and the completion of the border search, taking into account any additional facts and circumstances unique to the case. As such, ICE Special Agents are to document the progress of their searches, for devices and copies of information therefrom, and should consider the following factors:
  - a) The amount of information needing review;
  - b) Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;
  - c) Whether assistance was sought and the type of such assistance;
  - d) Whether and when ICE followed up with the agency or entity providing assistance to ensure a timely review;
  - e) Whether the traveler has taken affirmative steps to prevent the search of his or her property in a timely fashion; and
  - f) Any unanticipated exigency that may arise.

#### **8.4. Assistance by Other Federal Agencies and Non-Federal Entities.**

- 1) Translation, Decryption, and Other Technical Assistance.
  - a) During a border search, Special Agents may encounter information in electronic devices that presents technical difficulties, is in a foreign language, and/or encrypted. To assist ICE in conducting a border search or in determining the meaning of such information, Special Agents may demand translation, decryption, and/or technical assistance from other Federal agencies or non-Federal entities.
  - b) Special Agents may demand such assistance absent individualized suspicion.
  - c) Special Agents shall document such demands in appropriate ICE systems.

2) Subject Matter Assistance.

- a) During a border search, Special Agents may encounter information in electronic devices that are not in a foreign language or encrypted, or that do not require other technical assistance, in accordance with Section 8.4(1), but that nevertheless requires referral to subject matter experts to determine whether the information is relevant to the laws enforced and administered by ICE. For the purpose of obtaining such subject matter expertise, Special Agents may create and transmit a copy of such information to other Federal agencies or non-Federal entities.
- b) Special Agents may demand such assistance when they have reasonable suspicion of activities in violation of the laws enforced by ICE.
- c) Special Agents shall document such demands in appropriate ICE systems.

3) Demand Letter. Unless otherwise governed by a Memorandum of Understanding or similar mechanism, each demand for assistance is to be in writing (e.g., letter or email), approved by a supervisor, and documented in the appropriate ICE systems. Demands are to detail the context of the search requested, ICE's legal parameters regarding the search, retention, and sharing of any information found during the assistance, and relevant timeframes, including those described in this Directive.

4) Originals. For the purpose of obtaining subject matter assistance, Special Agents may create and transmit copies of information to other Federal agencies or non-Federal entities. Original electronic devices should be transmitted only when necessary to render the demanded assistance.

5) Time for Assistance and Responses Required.

- a) Assistance is to be accomplished within a reasonable period of time in order to preserve the status of the electronic devices and the integrity of the border search.
- b) It is the responsibility of the Special Agent demanding the assistance to ensure timely responses from assisting agencies or entities and to act in accord with section 8.3 of this Directive. In addition, Special Agents shall:
  - i) Inform assisting agencies or entities that they are to provide results of assistance as expeditiously as possible;
  - ii) Ensure that assisting agencies and entities are aware that responses to ICE must include any findings, observations, and conclusions drawn from their review that may relate to the laws enforced by ICE;

- iii) Contact the assisting agency or entity to get a status report on the demand within the first 30 calendar days;
- iv) Remain in communication with the assisting agency or entity until results are received;
- v) Document all communications and actions in appropriate ICE systems; and
- vi) Consult with a supervisor to determine appropriate action if the timeliness of results is a concern. If a demand for assistance is revoked, the Special Agent is to ensure all electronic devices are returned to ICE as expeditiously as possible.

#### **8.5. Retention, Sharing, Safeguarding, And Destruction.**

##### **1) By ICE**

- a) Seizure and Retention with Probable Cause. When Special Agents determine there is probable cause of unlawful activity—based on a review of information in electronic devices or on other facts and circumstances—they may seize and retain the electronic device or copies of information therefrom, or relevant portions thereof, as authorized by law.
- b) Retention of Information in ICE Systems. To the extent authorized by law, ICE may retain information relevant to immigration, customs, and other law enforcement matters in ICE systems if such retention is consistent with the privacy and data protection policies of the system in which such information is retained. For example, information entered into TECS during the course of an investigation will be retained consistent with the policies governing TECS.
- c) Sharing. Copies of information from electronic devices, or portions thereof, which are retained in accordance with this section, may be shared by ICE with Federal, state, local, and foreign law enforcement agencies in accordance with applicable law and policy. Sharing must be in compliance with the Privacy Act and applicable ICE privacy policies, such as the ICE Search, Arrest, and Seizure System of Records Notice.
- d) Safeguarding Data During Storage and Transmission. ICE will appropriately safeguard information detained, copied, retained, or seized under this directive while in ICE custody and during transmission to an outside entity. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking originals and copies to ensure appropriate disposition, and appropriate safeguards during transmission such as encryption of electronic data or physical protections (e.g., locked containers). Any suspected loss or compromise of information that contains personal data detained, copied, or seized under this directive must be reported immediately to the ICE Service Desk.



- e) Destruction. Copies of information from electronic devices, or portions thereof, determined to be of no relevance to ICE will be destroyed in accordance with ICE policy governing the particular form of information. Such destruction must be accomplished by the responsible Special Agent within seven business days after conclusion of the border search unless circumstances require additional time, which must be approved by a supervisor and documented in appropriate ICE systems. All destructions must be accomplished no later than 21 calendar days after conclusion of the border search.

## 2) By Assisting Agencies

- a) Retention during Assistance. All electronic devices, whether originals or copies of information therefrom, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to ICE.
- b) Return or Destruction. At the conclusion of the requested assistance, all electronic devices and data must be returned to ICE as expeditiously as possible. In the alternative, the assisting Federal agency may certify to ICE that any copies in its possession have been destroyed or it may advise ICE in accordance with Section 8.5(2)(c). In the event that any original electronic devices were transmitted, they must not be destroyed; they are to be returned to ICE.
- c) Retention with Independent Authority. 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 is of national security or intelligence value. In such cases, the retaining agency must advise ICE of its decision to retain certain information on its own authority. In the event that any original electronic devices were transmitted, the assisting Federal agency may make a copy of information therefrom for its retention; however, any originals must be returned to ICE.

## 3) By Non-Federal Entities

- a) ICE may provide copies of information from electronic devices to an assisting non-Federal entity, such as a private language translation or data decryption service, only for the period of time needed by that entity to render the requested assistance.
- b) Upon the completion of assistance, all copies of the information in the possession of the entity must be returned to ICE as expeditiously as possible. Any latent copies of the electronic data on the systems of the non-Federal entity must also be destroyed so that recovery of the data is impractical.

**8.6. Review, Handling, and Sharing of Certain Types of Information.**

- 1) Border Search. All electronic devices crossing U.S. borders are subject to border search; a claim of privilege or personal information does not prevent the search of a traveler's information at the border. However, the nature of certain types of information are subject to special handling by Special Agents, whether through policy or laws such as the Privacy Act and the Trade Secrets Act.
- 2) Types of Information
  - a) Business or Commercial Information. If, in the course of a border search, Special Agents encounter business or commercial information, such information is to be treated as business confidential information. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may specifically govern or restrict handling of the information, including criminal penalties for unauthorized disclosure.
  - b) Legal Information. Special Agents may encounter information that appears to be legal in nature, or an individual may assert that certain information is protected by the attorney-client or attorney work product privilege. If Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems.
  - c) Other Sensitive Information. Other possibly sensitive information, such as medical records and work-related information carried by journalists shall be handled in accordance with all applicable federal law and ICE policy. Although there is no Federal legal privilege pertaining to the doctor-patient relationship, the inherent nature of medical information warrants special care for such records. Questions regarding the review of these materials shall be directed to the ICE Office of the Chief Counsel and this consultation shall be noted in appropriate ICE systems.
- 3) Sharing. Information that is determined to be protected by law as privileged or sensitive is to be handled consistent with the laws and policies governing such information.

**8.7 Measurement.** ICE Headquarters will develop appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from ICE systems using data elements entered by Special Agents pursuant to this Directive.

- 8.8 Audit.** ICE Headquarters will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.
- 9. ATTACHMENTS.** None.
- 10. NO PRIVATE RIGHT STATEMENT.** This Directive is an internal policy statement of ICE. It is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees; or any other person.

Approved



John Morton  
Assistant Secretary  
U.S. Immigration and Customs Enforcement