

Policy Number: 10082.1
FEA Number: 360-112-002b


Office of the Director

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536

JUN 28 2012



**U.S. Immigration
and Customs
Enforcement**

MEMORANDUM FOR: Law Enforcement Personnel
FROM: John Morton
Director 
SUBJECT: Use of Public and Non-Public Online Information

Purpose

This memorandum provides U.S. Immigration and Customs Enforcement (ICE) law enforcement personnel guidance on the acceptable use of online information within the scope of their law enforcement duties.

Background

On December 8, 2010, Secretary Napolitano approved a decision memorandum titled, "Use of Public and Non-Public Online Information for Law Enforcement, Situational Awareness, and Intelligence Purposes," ("The Online Information Memorandum") that adopted a recommendation whereby the Department of Homeland Security (DHS), except members of the Intelligence Community governed by Executive Order 12333, would "follow the Department of Justice (DOJ) 1999 guidelines for online investigative and situational awareness activities." The Online Information Memorandum also suggested that DHS Components develop supplementary guidance, as necessary, for their mission-specific purposes consistent with DHS policy.

Discussion

Pursuant to the Online Information Memorandum, ICE law enforcement personnel should follow the below principles for the use of public and non-public online information, which have been adapted from the online investigative principles outlined in DOJ's 1999 Online Investigative Principles for Federal Law Enforcement Agents.¹

¹ Law enforcement personnel are ICE employees who conduct and support criminal, civil, and administrative law enforcement investigations and operations. Examples include special agents and other law enforcement officers, law enforcement investigative support personnel, intelligence research specialists, criminal research specialists, and attorneys prosecuting criminal, civil or administrative matters.

To implement these core principles, ICE directorates and program offices may establish guidance and/or modify existing guidance, as necessary, or reference the DOJ guidance as applicable to the activities in question.

ICE Principles for Law Enforcement Use of Public and Non-Public Online Information:

1. **Obtaining Information from Unrestricted Sources.** Law enforcement personnel may obtain information from publicly accessible online sources and facilities under the same conditions they may obtain information from other sources generally open to the public. This principle applies to publicly accessible sources located in foreign jurisdictions as well as those in the United States.
2. **Obtaining Identifying Information about Users or Networks.** There are widely available software tools for obtaining publicly available identifying information about a user or a host computer network. Law enforcement personnel may use such tools in their intended lawful manner under the same circumstances in which ICE guidelines and procedures permit them to look up similar identifying information (e.g., a telephone number) through non-electronic means. However, law enforcement personnel may not use software tools, even those generally available as standard operating system software, to circumvent restrictions placed on system users.
3. **Real-Time Communications.** Law enforcement personnel may passively observe and log real-time electronic communications open to the public under the same circumstances in which they may attend a public meeting.
4. **Accessing Restricted Sources.** Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into private space.
5. **Online Communications Generally.** Law enforcement personnel may use online services to communicate as they may use other types of communication tools, such as the telephone and the mail. Law enforcement personnel should retain the contents of a stored electronic message if they would have retained that message had it been written on paper. The contents should be preserved in a manner authorized by ICE procedures governing the preservation of electronic communications.
6. **Undercover Communications.** Law enforcement personnel communicating online with witnesses, subjects, or victims must disclose their affiliation with law enforcement when ICE guidelines would require such disclosure if the communication were taking place in person or over the telephone. Law enforcement personnel may communicate online under a non-identifying name or fictitious identity if ICE guidelines and procedures would authorize such communications in the physical world. For purposes of ICE undercover guidelines, each discrete conversation online constitutes a separate undercover activity or contact, but such a conversation may comprise more than one transmission between the law enforcement personnel and another person.

7. **Online Undercover Activities.** Just as law enforcement agencies may establish physical-world undercover entities, they also may establish online undercover facilities, such as bulletin board systems and Web sites, which covertly offer information or services to the public. Online undercover facilities, however, can raise novel and complex legal issues, especially if law enforcement personnel seek to use the system administrator's powers for criminal investigative purposes. Further, these facilities may raise unique and sensitive policy issues involving privacy, international sovereignty, and unintended harm to unknown third parties. Because of these concerns, a proposed online undercover facility, like any undercover entity, may be established only if the operation is authorized pursuant to ICE's guidelines and procedures for evaluating undercover operations.
8. **Communicating Online Through the Use of the Identity of a Cooperating Witness, with Consent.** Law enforcement personnel may ask a cooperating witness to communicate online with other persons in order to further an investigation if agency guidelines and procedures authorize such a consensual communication in person, over the telephone, or through other non-electronic means. Law enforcement personnel may communicate online using the identity of another person if that person consents, if the communications are within the scope of the consent, and if such activity is authorized by ICE guidelines and procedures. Personnel who communicate online through the identity of a cooperating witness are acting in an undercover capacity.
9. **Appropriating Online Identity.** "Appropriating online identity" occurs when law enforcement personnel electronically communicate with others by deliberately assuming the known online identity (such as the username) of a real person, without obtaining that person's consent. Appropriating identity is an intrusive law enforcement technique that should be used infrequently and only in serious criminal cases. When assuming an online identity, law enforcement personnel must follow all applicable ICE policies and guidelines.
10. **Activity by Law Enforcement Personnel during Personal Time.** While not on duty, law enforcement personnel are generally free to engage in personal online pursuits. If, however, the off-duty online activity directly and substantially relates to a law enforcement investigation, operation, or prosecution, law enforcement personnel are bound by the same restrictions regarding the use of online information as would apply when on duty.
11. **International Issues.** Unless gathering information from online facilities configured for public access, law enforcement personnel conducting investigations should use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction. Whenever an item or person is located abroad, law enforcement personnel should follow ICE's policies and procedures for international investigations.

Personnel who conduct and support criminal and civil law enforcement investigations and/or operations must adhere to the above principles when using information gathered online in support of an official agency criminal or civil law enforcement investigations and/or operations.

The principles that address the use of the Internet for undercover activities apply only to ICE personnel with the authority to conduct undercover investigations.

Personnel who conduct civil and criminal law enforcement activities for Enforcement and Removal Operations should also adhere to the above principles when using information gathered online in support of their law enforcement activities. Such personnel should remain mindful that the principles that address the use of the Internet for undercover activities apply only to those vested with such authority.

Attorneys with the Office of the Principal Legal Advisor should also adhere to the above principles, except those that are applicable to undercover activities, when using information gathered online in support of their handling of criminal, civil, or administrative matters.

No Private Right of Action

This memorandum is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter.