Privacy Requirements for Operational Use of Social Media

August 2019

U.S. Immigration and Customs Enforcement

ICE

Training Goals & Objectives

- To ensure ICE personnel understand and comply with the DHS Privacy Policy for Operational Use of Social Media (June 8, 2012)
  - § DHS Directive 110-01
  - § DHS Instruction 110-01-001
- This course covers:
  - § Key definitions
  - § Rules of Behavior for Law Enforcement and Non-Law Enforcement Activities

U.S. Immigration and Customs Enforcement

ICE

What Does This Policy Do?

- Regulates how DHS collects personally identifiable information (PII) from "Social Media" Internet sites for an "Operational Use"
- Requires DHS components and offices to establish Rules of Behavior that personnel must follow
- Requires annual training of all personnel who engage in this type of activity

U.S. Immigration and Customs Enforcement

ICE

Why Was This Policy Created?

- To address public and congressional concerns about how DHS collects PII from Social Media
- To ensure DHS is not engaging in an unlawful or inappropriate collection of PII from Social Media
- To ensure that there are clear "dos and don'ts" for personnel to follow these are called the "Rules of Behavior"
- To ensure all DHS personnel are aware of the rules through annual training

gration
ms
Enforcement

ICE

Applicable Laws

The Privacy Act of 1974

- A code of practices for the collection, maintenance, use, and dissemination of information about individuals

The Electronic Communications Privacy Act (1986)

- Law Enforcement requires a court order to intercept private electronic communications in real time

The Stored Communications Act (1986)

- Creates Fourth Amendment-like privacy protection for digital communications stored on the internet.
- It limits the ability of the government to compel an ISP to turn over content information and non-content information

Other Country Privacy Laws

U.S. Immigration and Customs Enforcement

ICE

What is the "Operational Use" of "Social Media"?

When DHS is collecting PII about individuals from a Social Media site for the purpose of:

- Investigating them (criminal, civil, or administrative)
- Making a benefit decision about them
- Making a personnel or suitability decision about them
- Enhancing situational awareness (to support incident management decision making)
- Any other official purpose that potentially may affect their rights, privileges, or benefits

DHS Instruction 110-01-001, Section IV.D.

U.S. Immigration and Customs Enforcement

ICE

This Policy Does Not Apply To:

- Agency use of Social Media for communications and outreach to the public
- Personnel use of Social Media for professional development, such as training and continuing education
- Use of Social Media to facilitate internal meetings
- Use of internal DHS intranets or applications
- Use of search engines for general Internet research

U.S. Immigration and Customs Enforcement

ICE

What is Personally Identifiable Information (PII)?

"Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

DHS Instruction 110-01-001, Section IV.E.

U.S. Immigration and Customs Enforcement

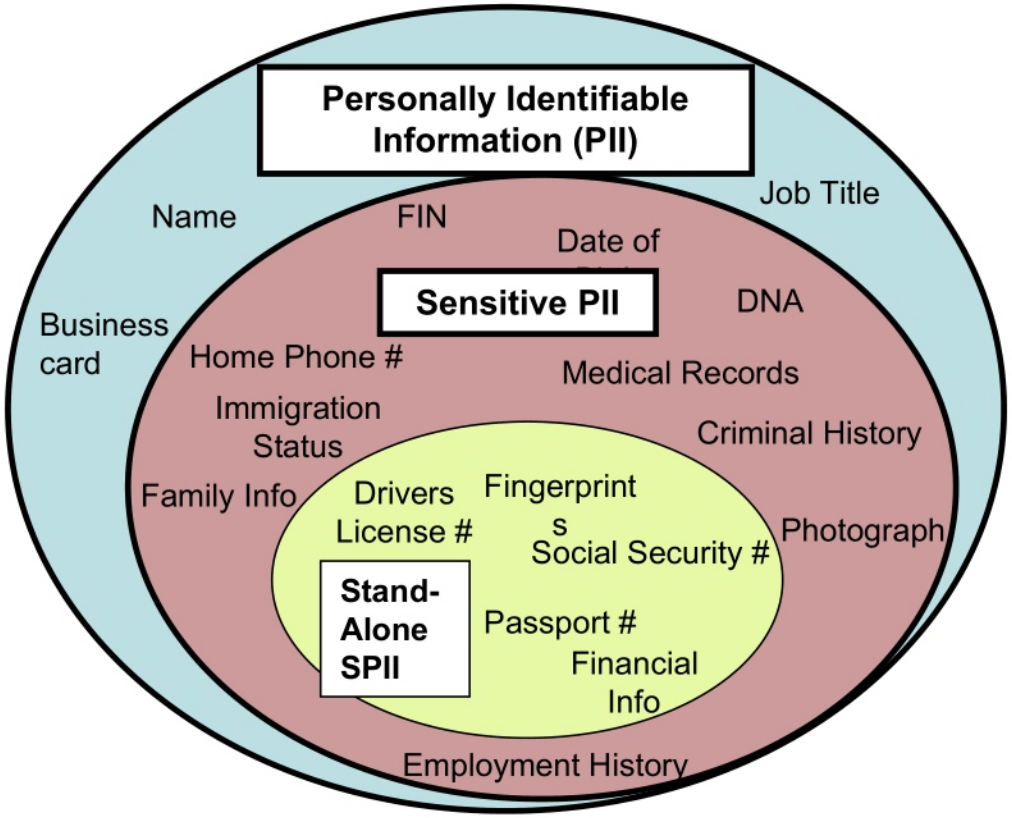
ICE

Who You Are

ID Numbers

Biometrics

Other Info About You



*This is not a comprehensive list.
**See the Handbook on Safeguarding Sensitive PII at DHS available on the ICE Privacy intranet site for more information.

U.S. Immigration and Customs Enforcement

ICE

What is "Social Media"?

"The sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact."

YouTube

Instagram

"This definition does not apply to internal Department intranets or applications."

DHS Instruction 110-01-001, Section IV.K.

U.S. Immigration and Customs Enforcement

ICE

How Do I Know When I Am on a "Social Media" Site Online?

- Because of the trend toward including interactive, Social Media-type features on "regular" Internet sites, it is often hard to know if you are on a "regular" Internet site or a "Social Media" site

U.S. Immigration and Customs Enforcement

ICE

How Do I Know When I Am on a "Social Media" Site Online?

- Because ICE's Rules of Behavior apply to all online activity where you collect PII, you do not have to be concerned about whether you are on a Social Media site, or a regular Internet site
- Simply follow the appropriate Rules of Behavior *anytime* you collect PII online:
  - Collection for a law enforcement purpose – follow the ICE Law Enforcement Rules of Behavior
  - Collection for a non-law enforcement purpose – follow the ICE Non-Law Enforcement Rules of Behavior

U.S. Immigration and Customs Enforcement

ICE

U.S. Immigration and Customs Enforcement

ICE Rules of Behavior (ROB) for Non-Law Enforcement Activities

ICE

ICE ROB for Online Non-Law Enforcement Activities

- Established in a Memorandum from John Morton to ICE Personnel, *Use of Public Online Information for Non-Law Enforcement Work-Related Activities* (June 28, 2012)

(b)(7)(E)

U.S. Immigration and Customs Enforcement

ICE

ICE Rules of Behavior (ROB) for Online Law Enforcement Activities

U.S. Immigration and Customs Enforcement

ICE

ICE ROB for Online Law Enforcement Activities

- Established in a Memorandum from John Morton to Law Enforcement Personnel, *Use of Public and Non-Public Online Information* (June 28, 2012)

(b)(7)(E)

- Based on and consistent with the DOJ Online Investigative Principles for Federal Law Enforcement Agents (1999)

U.S. Immigration and Customs Enforcement

ICE

ICE ROB for Online Law Enforcement Activities

- Apply to any ICE personnel conducting law enforcement activities:
  - § Where PII is collected
  - § For a law enforcement purpose
  - § From the Internet
- Apply to ICE law enforcement and other support personnel engaging in a civil, criminal, or administrative law enforcement investigation, operation, or activity
  - § Includes attorneys prosecuting criminal, civil or administrative matters

U.S. Immigration and Customs Enforcement

ICE

ICE ROB for Online LE Activities: Requirements

- Obtaining information from unrestricted sources
  - § You may obtain information from publicly accessible online sources under the same conditions you may obtain information from other sources generally open to the public.

- Accessing restricted sources
  - § You may not access restricted online sources absent legal authority permitting entry into private space.

U.S. Immigration and Customs Enforcement

ICE

ICE ROB for Online LE Activities: Requirements

- Obtaining identifying information about users or networks
  - You may use software tools to obtain PII about a user or host computer network under same circumstances in which ICE guidelines and procedures allow you to look up similar information such as a phone number.
  - You may not use software tools to circumvent restrictions placed on system users.
- Real time communications
  - You may passively observe and log real-time electronic communications open to the public under the same circumstances in which you may attend a public meeting.

U.S. Immigration and Customs Enforcement

ICE

ICE ROB for Online LE Activities: Requirements

- Online communications
  - § Law enforcement 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 only if ICE guidelines and procedures would authorize such communications in the physical world.

U.S. Immigration and Customs Enforcement

ICE

ICE ROB for Online LE Activities: Requirements

- 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 usemame) 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.

U.S. Immigration and Customs Enforcement

ICE

ICE ROB for Online LE Activities: Requirements

Record Retention

- Retain contents of a stored electronic message if you would have retained that message had it been written on paper.

- International Issues

- Unless gathering information from online facilities configured for public access, e.g., Facebook, law enforcement personnel conducting investigations should ascertain whether any pertinent computer system, data, 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.

U.S. Immigration and Customs Enforcement

ICE

U.S. Immigration and Customs Enforcement

Contact & Resource Information

Questions? Contact the ICE Privacy & Records Office, Privacy Branch

(202) 732-3300

ICEPrivacy@ice.dhs.gov

Website:

(b)(7)(E)

Links:

ICE Law Enforcement Rules of Behavior

(b)(7)(E)

ICE Non-Law Enforcement Rules of Behavior

(b)(7)(E)

U.S. Immigration and Customs Enforcement

ICE