situational awareness and investigating an individual in a criminal, civil, or administrative context. Under Section 2.2.4 Rules of Behavior, the Handbook states that limited social media use is permitted to support component missions when in compliance with Component Privacy Officers' Rules of Behavior. The CIU will ensure compliance with Rules of Behavior as discussed below.

Discussion

(b)(7)(E)

Until recently, it was not necessary to establish an account to log into online platforms to view information made available to the public by individual account holders. Interests of these online platforms have evolved, and the companies are increasingly motivated by financial interests to identify online users for advertising data, location data, and search habits. The entities seeking and funding the collection of user data are often averse to law enforcement, to the U.S. government, or to the United States as a whole. To facilitate the financial and programmatic gains in collecting user information, online application companies now require the user to establish an account to view information account holders have designated as publicly available.

Because of the trend toward including interactive, social media-type features on "regular" internet sites, it is often hard for the user to know if they are on a "regular" internet site or a "social media" site. Use of an unattributable browser is beneficial even when searching open source information on the internet because of the inherent risk related to internet "bots" that run automated tasks (scripts). Research indicates that more than half of all web traffic is generated by bots. Some bots are "good" and handle tasks like reporting weather or sports scores. Other bots are "malicious" self-propagating malware that infect the host and connect back to a central server(s). The server functions as a "command and control center" for a botnet or a network of compromised computers and similar devices (*reference: https://us.norton.com/internetsecurity-malware-what-are-bots.html*). These malicious bots, imbedded by bad actors, are often designed to target and search out law enforcement or government activities, interests, and personnel. (b)(7)(E)

(b)(7)(E)

Historically, to accommodate unattributed access to the internet, ICE offices purchased standalone computers through the Office of the Chief Information Officer (OCIO) which connected to the internet through commercial internet service providers and generated one-time costs (purchase of the computer hardware devices) and recurring monthly fees (for internet service). The requested unattributable browser service provides safeguards and conveniences not offered through the utilization of a standalone computer. The unattributable browser service licensee accesses the internet in their normal workspace

without the disruption of moving back and forth between normal workspace and the standalone computer. Product licensing of the unattributable browser service includes audit functions through an Administrative Console. Each upload, download, and browsing session will reside in the Administrative Console cloud. All historical log data for user behavior will be tracked and saved in the Administrative Console. The licensing entity will provide an encryption key to access the historical log data which will be maintained for a period of 90 rolling days (after which time, the information will be deleted). With the encryption key, historical logs can be viewed and/or downloaded through the Administrative Console. The licensing entity will not have access to the historical cloud data maintained in the Administrative Console. The licensing entity will assign a Program Manager to assist in the implementation and management of the unattributable browser and with on-going ICE requirements.

The CIU will comply with the following Rules of Behavior, and others as deemed appropriate, for its operational use of social media:

Equipment: The unattributable browser service application will be installed by OCIO and accessed on government-issued equipment. The term "equipment" includes both non-portable devices such as desktop computers as well as mobile devices such as laptop computers, smartphones, and tablets.

(b)(7)(E)

Public Interaction: CIU personnel will access publicly available information through social media only by reviewing posted information without interacting with any individual who posted the information.

Privacy Settings: CIU personnel will respect individuals' privacy settings and access only information that is publicly available unless the individual whose information the employee seeks to access has given consent to access it.

PII Collection: CIU personnel will collect the minimum PII necessary for the proper performance of their authorized duties. The Privacy Act requirement in 5 U.S.C. 552a(e)(1) normally limits agencies to collecting only information about individuals relevant and necessary to accomplish a purpose of the agency required by statute or Executive Order. The (e)(1) requirement also allows an exemption, which is applicable to the intended CIU use, when it is necessary to ensure the integrity of law enforcement efforts.

PII Safeguards: CIU personnel will protect PII as required by the Privacy Act and DHS privacy Policy.

Documentation: ICE's rules of behavior state that law enforcement personnel should retain the information they access on the internet, including social media, if they would have retained that content had it been written on paper. Content will be preserved in a manner authorized by ICE procedures governing the preservation of electronic communications.