

DEPARTMENT OF HOMELAND SECURITY
UNITED STATES SECRET SERVICE
WASHINGTON, D.C. 20223

Freedom of Information and Privacy Acts Branch
Communications Center
245 Murray Lane, S.W.
Building T-5
Washington, D.C. 20223

Electronic Frontier Foundation
454 Shotwell Street
San Francisco, Ca 94110
Attn: James Tucker & Shane Witnov

File Number: 20090806 - 20090813

Dear Requester:

This letter is intended to acknowledge the receipt of your recent Freedom of Information/Privacy Acts request received by the United States Secret Service on October 8, 2009, for information pertaining to the following:

File No.: 20090806 – Documents that contain information on the use of “fake” identities to “trick” users “into accepting a government official as a friend” or otherwise provide information to the government as described in the Boston Globe article;

File No.: 20090807 – Guides, manuals, policy statements, memoranda, presentations, or other materials explaining how government agents should collect information on social-networking websites;

File No.: 20090808 – Guides, manuals, policy statements, memoranda, presentations, or other materials detailing how or when government agents may collect information through social-networking websites;

File No.: 20090809 – Guides, manuals, policy statements, memoranda, presentations, or other materials detailing what procedures government agents must follow to collect information through social-networking websites;

File No.: 20090810 – Guides, manuals, policy statements, memorandum, presentations, agreements (both formal and informal) with social-networking companies, or other materials relating to “privileged user” access by the Secret Service to social-networking websites;

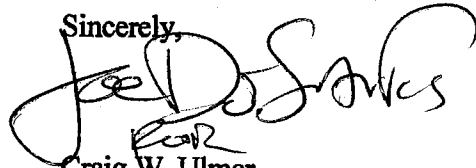
File No.: 20090811 – Guides, manuals, memoranda, presentations or other materials for using any visualization programs, data analysis programs or tools used to analyze data gathered from social networks;

File No.: 20090812 – Contracts, requests for proposals, or purchase orders for any visualization programs, data analysis programs or tools used to analyze data gathered from social networks; and

File No.: 20090813 – Guides, manuals, policy statements, memoranda, presentations, or other materials describing how information collected from social-networking websites is retained in government databases or shared with other government agencies.

Enclosed are documents responsive to your request. The documents are being released in their entirety. No deletions or exemptions have been claimed.

Sincerely,

A handwritten signature in black ink, appearing to read "Craig W. Ulmer". The signature is stylized and cursive, with a large initial "C" and "U".

Craig W. Ulmer
Special Agent In Charge
Freedom of Information &
Privacy Acts Officer

Enclosure(s)

INTERNET USE POLICY

General Information

Purpose

This directive defines the responsibilities of Secret Service employees with respect to the appropriate use of the Internet and the services it provides.

Scope

This directive applies to all Secret Service facilities and computer systems, regardless of location; and to all Secret Service personnel, including contract personnel employed by the Secret Service.

Definition of Terms

Firewall - A combination of computer hardware and software that screens incoming data in order to guard against unauthorized system intrusion.

Internet - The Internet, or 'Net,' is a public global network. Originally developed to link computer systems within the Department of Defense in the 1970s, the system was later expanded by the National Science Foundation to include colleges, research institutions and other U.S. Government agencies. In 1991, the development of the World Wide Web made the Internet easily accessible to the general public. Today, the Internet is a broad collection of networks mostly run by large telecommunications companies.

Internet Service Provider (ISP) - A vendor who provides direct access to the Internet, usually for a fee. An ISP normally provides its users a Web Browser and an e-mail account.

Secret Service Computers - For the purposes of this Directive, a Secret Service computer is defined as any computer owned or leased by the Secret Service (regardless of location), or any other computer being used for Secret Service business.

Stand Alone Computer - A computer that is not connected to any Secret Service information system and which would not require the transference of data from this computer to other Secret Service computers. For Internet use, the stand alone computer's data storage devices must be devoid of Secret Service data.

Web Browser - A Web browser/browser is a software tool used to locate and view data in a standardized graphical format on the WWW (e.g., Netscape Navigator).

World Wide Web (WWW) -The WWW or 'Web' is a portion of the information available on the Internet and consists of an electronic collection of documents stored on computers worldwide. The Web is noted for its graphics (photos, colors, etc.) and hyperlinks (allow users to jump quickly from one document to another).

Responsibilities

OFFICE OF PROTECTIVE RESEARCH - Information Resources Management Division (IRM) - IRM controls connections to the Internet, and manages all services associated with the Internet.

ASSISTANT DIRECTORS/CHIEF COUNSEL - Assistant Directors or the Chief Counsel has ultimate authority to grant or deny employee access to the Internet.

ASSISTANT DIRECTOR (INV, OPR) - The appropriate Assistant Director (INV, OPR) will review and approve on a case by case basis all requests for Internet access/use to support ongoing investigations.

OFFICE SUPERVISORS - Office supervisors may limit or revoke the privilege for their employees to use Secret Service equipment to access the Internet for personal non-government usage.

OFFICE SECURITY REPRESENTATIVE (OSR) - The OSRs within each office are responsible for coordinating computer security issues with IRM Information Security (INFOSEC) personnel. OSRs are responsible for installing and updating anti-virus software on all computers connected to the Internet.

Authorization

All Secret Service employees have access to the Internet through the Secret Service Network.

Internet Connectivity

The Secret Service Network is equipped with safeguards, such as firewalls and intrusion detection systems, to minimize the possibility of computer virus exposure or intrusion by unauthorized personnel. Internet connectivity must be achieved via the Secret Service Network, unless specifically authorized in accordance with the Investigative Use section of this policy.

The Information Resources Management Division (IRM) controls the connections to the Internet. It is the only entity which may connect (or direct the connection of) Secret Service equipment to the Internet service. Only IRM approved "connectivity" software may be utilized.

Anti-virus software must be installed, updated and activated in any computer connected to the Internet, in accordance with policy in this manual regarding Baseline Security Controls for Personal Computer Virus Protection.

Personal and Inappropriate Uses

Secret Service employees are permitted limited use of Secret Service equipment to access the Internet for personal needs.

Employees are expected to conduct themselves professionally in the workplace and to refrain from using government office equipment for activities that are inappropriate.

Employees are expected to refer to directive Human Resources and Training Manual section PER-05(10), "Use of Government Systems," for information regarding personal use, no right to privacy, privilege, employee non-work time, inappropriate personal uses, and sanctions for misuse.

Investigative Use

Criminal investigations that involve Internet technology currently fall into two broad categories:

- Threats against Secret Service protectees.
- Violations of Title 18 USC Section 1030 (Fraud and Related Activity in Connection with Computers), and related statutes. (See "section CFI-03, Computer Fraud Investigations Manual.")

Requests for Internet access/use to support ongoing investigations will be reviewed by the appropriate Assistant Director (INV, OPR), and approved on a case by case basis.

Personnel utilizing the Internet for investigative purposes are reminded that the access of an Internet site leaves an "electronic footprint," which can generally be used to identify the Internet address of the entity accessing the site. Therefore, all Internet accesses for investigative use will utilize 'stand-alone' computers that use anonymous accounts from an ISP.

The Electronic Crimes Special Agent Program (ECSAP) in Financial Crimes Division is available to assist field offices with their Internet investigations, as well as the seizure and forensic processing of computers encountered during investigations.

Many law enforcement organizations have established Home Pages, which allow for the exchange of investigative information via Internet e-mail. Internet e-mail is not secure. Due to the possibility of interception, sensitive investigative information or data should not be transmitted via Internet e-mail.

Disclosure

Executive Branch employees do not have a right or expectation of privacy while using any government office equipment at any time, including accessing the Internet, using e-mail, or for limited personal use. To the extent that employees wish that their private activities remain private, they should avoid using an Agency's office equipment, such as their computer, the Internet, or e-mail "for personal use." By using government office equipment, executive branch employees imply their consent to disclosing the contents of any encrypted files.

By using this office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet, using e-mail, or for limited personal use. Any use of government communications resources is made with the understanding that such use is generally not secure and is not anonymous.

All e-mail messages (and other electronic database information) as defined in Federal Law, are government records. Electronic communications may be disclosed within an Agency to employees who have a need to know in the performance of their duties. Agency officials, such as system managers and supervisors, may access any electronic communications for work-related purposes. Electronic communications may only be disclosed externally in accordance with applicable law or regulations.