DEPARTMENT OF DEFENSE
OFFICE OF GENERAL COUNSEL
1600 DEFENSE PENTAGON
WASHINGTON, DC 20301-1600

06 Feb 2001

MEMORANDUM

SUBJECT: Principles Governing the Collection of Internet Addresses by DOD Intelligence and Counterintelligence Components

This document lays the initial groundwork for determining how to apply intelligence oversight principles to the conduct of intelligence/counterintelligence (FI/CI) activities on the Internet. It is not intended to provide comprehensive intelligence oversight guidance. On the contrary, this paper only addresses a single question – *Does obtaining an e-mail or site address constitute a collection of information about a United States Person?*

These Principles provide a framework for answering this question. They are not a substitute for conducting a case-by-case analysis nor are they directive. Instead, they are intended to serve as a tool to assist the attorney and the intelligence officer in determining how to proceed during a given Internet-based activity. It is the expectation of this office that individual FI/CI components will build upon these principles to establish internal guidelines.

While these Principles are being distributed by the Office of General Counsel, they represent the work and collective wisdom of attorneys and intelligence experts from throughout the Department of Defense, including the Office of the Assistant to the Secretary of Defense for Intelligence Oversight, the National Security Agency, the Defense Intelligence Agency, the Defense Information Systems Agency, the Joint Staff, USSPACECOM, and each of the Military Services.

Original signed
Richard L. Shiffrin
Deputy General Counsel
(Intelligence)

Principles Governing the Collection of Internet Addresses by DOD Intelligence and Counterintelligence Components

Increasingly, DOD intelligence components are conducting intelligence and counterintelligence activities on the Internet. One challenge they confront is to maximize the use of the Internet while ensuring that such use complies with Executive Order 12333, *United States Intelligence Activities,* and its implementing regulation, DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons.*[1] Despite the fact that both of these documents were published well before the development of the Internet as it exists today, the concepts, principles, and procedures they embody remain vibrant and govern the intelligence and counterintelligence use of the Internet.

In order to properly apply the provisions of E.O. 12333 and DOD 5240.1-R to the use of the Internet, intelligence and counterintelligence personnel need to know how to analyze, as well as characterize, IP addresses, URLs, and e-mail addresses. All three of these categories of information present challenges that are different from those encountered when working with traditional forms of information. Yet all three fit well within the framework of DOD 5240.1-R. A discussion of each of the three categories follows.

IP Addresses

An IP address is a numeric string (e.g., 149.122.3.30) that identifies a hardware connection on a network. The numeric string is information about the owner, operator, or user of the hardware connection. As is the case with a telephone number, the numeric string comprising an IP address does not, without further information, identify or consist of information about a United States person. However, open source information about IP addresses is available on the web. Sometimes, the information that is available is very general and would not allow one to determine if the IP address is information about a U.S. person. In other instances, the information that is available is quite specific and would allow such a determination.[2]

Intelligence and counterintelligence (FI/CI) components are not necessarily required to try to decipher an IP address as soon as they encounter one. They are only required to engage in such an inquiry once a decision is made to conduct analysis that is focused upon specific IP addresses. Prior to such analysis, IP addresses may be treated as "data acquired by electronic

[1] The stated purpose of these documents is to enable intelligence components to effectively carry out their authorized functions while ensuring that any activities that affect U.S. persons are conducted in a manner that protects the constitutional rights and privacy of such persons.

[2] Even if a "look-up" site reveals that an IP address is assigned to a U.S. service provider, that is not necessarily sufficient information to require a presumption that the address is associated with a United States person. In the sense that a telephone number gives more information about the caller than about the phone company, the IP address gives more information about the individual connection than about the service provider that is facilitating that connection. Nevertheless, some service providers, for example Erols, principally provide service to a U.S.-based clientele. An IP address within a block assigned to such an ISP might merit the presumption that any IP address within that block identifies a U.S. person. Conversely, if a group of IP addresses is known to be assigned to a non-U.S. person (e.g., a foreign corporation), then the FI/CI component may presume that any given IP address within that block is associated with a non-U.S. person.

means." In accordance with DOD 5240.1-R, procedure 2.B.1, such data is not considered to be collected until it has been processed into intelligible form. There are no intelligence oversight restrictions on the maintenance or disposition of information that is not considered to have been "collected."

However, once the decision is made to conduct analysis focused upon specific IP addresses, the "collecting" component is obliged to conduct a reasonable and diligent inquiry to determine whether any of the IP addresses are associated with United States persons.[3] To conduct this inquiry, the component may use the above described web tools, but also must consider any external information available to it that might assist in identifying the IP address. If the FI/CI component still cannot reasonably determine whether any given IP address is associated with at U.S. person, then it may apply the presumption that unattributed IP addresses do not constitute information about a person and the IP address may be the subject of inquiry without regard to whether or not it is associated with a U.S. person. If, however, the component subsequently obtains information to indicate that an IP address is associated with a U.S. person, then the presumption is overcome and that IP address must be handled in accordance with the procedures governing the collection of information about U.S. persons.[4] The collecting component should document the efforts made to determine whether the IP address in question is associated with a U.S. person.

E-Mail Addresses

An e-mail address identifies a user so that the user can receive Internet e-mail. An e-mail address typically consists of a name to identify the user to the mail server, followed by "@" and the host name and domain name of the mail server. For example, if Anne E. Oldhacker has an account on the mail server called baz at Foo Enterprises, she might have an e-mail address, aeo@baz.foo.com.

E-mail addresses, unlike both IP addresses and URLs, are nearly universally associated with individuals. It is often difficult, however, to identify the individual with whom any given e-mail address is associated. Some e-mail addresses are configured as a string of alphanumeric symbols that do not convey any meaningful information (e.g. aronssop@ or smi2345@). Others plainly identify an individual (e.g. patti.aronsson@). Regardless of how straightforward an e-mail address appears to be on its face, more often than not, it does not provide sufficient

[3] The following is an example of when the requirement is triggered:

A counterintelligence component may maintain a database of all IP addresses that have attempted to gain unauthorized access into or information about DOD computers, without regard to whether or not any given IP address is associated with a United States person, and also may conduct statistical analysis of the intruding IP addresses. However, as soon as the CI component decides to investigate whether some subset of these intrusions represents an attack by a foreign intelligence service, the CI component is obliged to conduct an inquiry to try to determine whether any of the IP addresses within that subset are associated with United States persons.

[4] Information that identifies a U.S. person may be collected by an intelligence or counterintelligence component only if it is necessary to the conduct of a function assigned the component, and only if it falls within one of the thirteen categories listed in DOD 5240.1-R, Procedure 2, Paragraph C, "Types of Information That May Be Collected About United States Persons." Additional limitations are imposed in Procedures 5 through 10 on the use of specific collection techniques.

information to identify it as being affiliated with a United States person. Sometimes, though, the name to the left of the "@" will provide persuasive evidence that the e-mail address is associated with a U.S. person; for example, the person may be a well known public figure or may be the target of an investigation or inquiry in which the intelligence investigator or analyst is engaged.

Occasionally, the information to the right of the "@" may provide persuasive evidence about whether an e-mail address is associated with a U.S. person. The information to the right of the "@" represents the service provider. Some service providers predominately serve a non-U.S. based clientele and e-mail accounts with such providers may be presumed not to be U.S. person accounts. Other service providers are so closely affiliated with the U.S. that any e-mail account with that provider should be presumed to be associated with a U.S. person (e.g. aronssop@osdgc.osd.mil).

This latter category of e-mail addresses may only be collected, retained, or disseminated in accordance with the requirements of DOD 5240.1-R. All other e-mail addresses may be treated in a manner similar to the approach described for the treatment of IP addresses. E-mail addresses that are not self-evidently associated with U.S. persons may be acquired, retained and processed by CI and FI components without making an effort to determine whether any given address is associated with a United States person so long as the component does not engage in analysis focused upon specific addresses. Once such analysis is initiated, the CI or FI component must make an effort to determine whether the addresses are associated with U.S. persons.

Unlike IP addresses, there is no central repository of e-mail addresses to assist the component in identifying them. Instead, the component must rely principally upon traditional methods to try to determine whether any a given address is being used by a United States person. Oftentimes, particularly for those e-mail addresses which are cryptic, it will be virtually impossible for the CI or FI component to make a determination. In such instances, the component may presume that the e-mail addresses do not identify U.S. persons. As with all presumptions, however, the component is under a continuing obligation to be alert to information that might overcome the presumption.

URLs

URL (Uniform Resource Locator) is a standard way of specifying the location of an object on the Internet, typically a web page. URLs are the form of address used on the World Wide Web. URLs typically appear as words rather than numbers and, while some URLs are gibberish, most of them convey a modicum of information. In some instances, that information is of a character that ostensibly identifies a person (e.g. Mary_Smith.com or USSTEEL.com). In other instances, the words in a URL do not convey, in any apparent way, information concerning persons (e.g. Bicyclists.com).

Unlike IP addresses or e-mail addresses, URLs are, almost by definition, publicly available. As such, even if they identify U.S. persons,[5] lists of URL addresses may be maintained

[5] In determining whether a URL identifies a U.S. person, a key factor to consider is the information to the right of the dot (the domain). If the domain is one commonly associated with a foreign country (e.g. .uk, .fr), then, in the absence of contrary information, the URL can be presumed to identify a non-U.S. person. Conversely, if the domain

by CI/FI components provided such collection is within the scope of an authorized intelligence/counterintelligence activity assigned to that component. CI/FI components also may open the websites associated with such URLs if doing so is part of an authorized mission. If, however, the component wants to collect information beyond that which is available on the site, then it must make an effort to determine whether the person about whom they are collecting is a U.S. person and, if so, comply with the requirements of DOD 5240.1-R.[6]

---

is associated with the United States (e.g., .gov, .mil), then the URL should be presumed to be information that identifies a U.S. person. Several domains are universally available, such as .com, .net and .org, and thus do not inform the determination about whether or not the URL identifies a U.S. or a foreign person. The mere use of a name in association with a universally available domain is usually insufficient to trigger the presumption that the URL constitutes information that identifies a U.S. person. As with all information, though, if information is obtained to indicate the URL is associated with a U.S. person, then the further collection, retention, and dissemination of the URL name must be handled in accordance with DOD 5240.1-R.

[6] This discussion does not address those web sites that limit access to subscribers or in some other manner are not available to the public.