U.S. Department of Justice

Criminal Division

Office of Enforcement Operations *Washington, D.C. 20530*

CRM-200401104

Mr. Chris Hoofnagle
Legislative Counsel
epic.org
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009

SEP 3 2004

Dear Mr. Hoofnagle:

In connection with your Freedom of Information act request dated June 22, 2001, on behalf of your client, the Electronic Privacy Information Center, the Office of Intelligence Policy and Review referred one document, a fifty-seven page report entitled "Online Investigative Principles for Federal Law Enforcement Agents," to this Office for processing and response to you. Although it is uncertain whether this document is, in fact, genuinely responsive to your request for "records relating to transactions, communications and contracts concerning businesses that sell individuals' personal information," in the interest of completeness we have decided to process it and provide you with nonexempt portions.

We are withholding portions of this document pursuant to the following FOIA exemptions set forth in 5 U.S.C. 552(b):

(2) which permits the withholding of information relating solely to the internal personnel rules and practices of an agency;

(7) which permits the withholding of records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information...

(e) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law;

Please be advised that Principle 7 (pages 34-40) and Principle 9 (pages 44-48) are being withheld in full pursuant to the above-cited exemptions. All other information partially withheld likewise pertains solely to these two principles.

Although I am aware that you have filed litigation on behalf of your client regarding these records I am required to inform you of your right to an administrative appeal.

You have a right to an administrative appeal of this denial of your request. Department regulations provide that such appeals must be filed within sixty days of your receipt of this letter. 28 C.F.R. 16.9. Your appeal should be addressed to: The Office of Information and Privacy, United States Department of Justice, Flag Building, Suite 570, Washington, D.C. 20530. Both the envelope and the letter should be clearly marked with the legend "FOIA Appeal.

If you elect to file an appeal, please include, in your letter to the Office of Information and Privacy, the Criminal Division file number that appears above your name in this letter.

Sincerely,

Thomas J. McIntyre, Chief
Freedom of Information/Privacy Act Unit
Office of Enforcement Operations
Criminal Division

ONLINE INVESTIGATIVE PRINCIPLES FOR FEDERAL LAW ENFORCEMENT AGENTS

PREPARED BY:

THE ONLINE INVESTIGATIONS
WORKING GROUP

Final Version (November 1999)

TABLE OF CONTENTS

APPENDIX B

THE ONLINE INVESTIGATIVE PRINCIPLES

[Although these Principles are intended to state the basic rule for each major category of investigative activity, the Commentary that follows each Principle in the body of this document includes important legal and practical considerations pertaining to the investigative activity that the Principle describes. Accordingly, the reader is advised to read both the relevant Principle and the accompanying Commentary before undertaking the specific online investigative activity described.]

PART I
PRINCIPLES GOVERNING OBTAINING INFORMATION

PRINCIPLE 1
OBTAINING INFORMATION FROM UNRESTRICTED SOURCES

Law enforcement agents may obtain information from publicly accessible online sources and facilities under the same conditions as 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.

PRINCIPLE 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 on a network. Agents may use such tools in their intended lawful manner under the same circumstances in which agency rules permit them to look up similar identifying information (e.g., a telephone number) through non-electronic means. However, agents may not use software tools – even those generally available as standard operating system software – to circumvent restrictions placed on system users.

PRINCIPLE 3
REAL-TIME COMMUNICATIONS

An agent may passively observe and log real-time electronic communications open to the public under the same circumstances in which the agent could attend a public meeting.

PRINCIPLE 4
ACCESSING RESTRICTED SOURCES

Law enforcement agents may not access restricted online sources or facilities absent legal authority permitting entry into private space.

PART II
PRINCIPLES GOVERNING COMMUNICATIONS ONLINE

PRINCIPLE 5
ONLINE COMMUNICATIONS – GENERALLY

Law enforcement agents may use online services to communicate as they may use other types of communication tools, such as the telephone and the mail. Law enforcement agents should retain the contents of a stored electronic message, such as an e-mail, if they would have retained that message had it been written on paper. The contents should be preserved in a manner authorized by agency procedures governing the preservation of electronic communications.

PRINCIPLE 6
UNDERCOVER COMMUNICATIONS

Agents communicating online with witnesses, subjects, or victims must disclose their affiliation with law enforcement when agency guidelines would require such disclosure if the communication were taking place in person or over the telephone. Agents may communicate online under a non-identifying name or fictitious identity if agency guidelines and procedures would authorize such communications in the physical world. For purposes of agency undercover guidelines, each discrete online conversation constitutes a separate undercover activity or contact, but such a conversation may comprise more than one online transmission between the agent and another person.

PRINCIPLE 7

b2
b7E

b2
b7E

PRINCIPLE 8
COMMUNICATING THROUGH THE ONLINE IDENTITY OF A COOPERATING WITNESS, WITH CONSENT

Law enforcement agents may ask a cooperating witness to communicate online with other persons in order to further a criminal investigation if agency guidelines and procedures authorize such a consensual communication over the telephone. Law enforcement agents may communicate using the online 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 agency guidelines and procedures. Agents who communicate through the online identity of a cooperating witness are acting in an undercover capacity.

PRINCIPLE 9

b2
b7E

b2
b7E

PART III: OTHER ISSUES

PRINCIPLE 10
ONLINE ACTIVITY BY AGENTS DURING PERSONAL TIME

While not on duty, an agent is generally free to engage in personal online pursuits. If, however, the agent's off-duty online activities are within the scope of an ongoing investigation or undertaken for the purpose of developing investigative leads, the agent is bound by the same restrictions on investigative conduct as would apply when the agent is on duty.

PRINCIPLE 11
INTERNATIONAL ISSUES

Unless gathering information from online facilities configured for public access, law enforcement agents conducting online investigations should use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction. Whenever any one of these is located abroad, agents should follow the policies and procedures set out by their agencies for international investigations.

OVERVIEW

A. The Need for Guidance[1]

The rapid growth of publicly accessible computer networks – most notably the Internet – is changing the work of federal law enforcement agents. To an ever greater extent, they are being called upon to:

- Investigate attacks on the confidentiality, integrity, and availability of computer networks and data;
- Investigate other crimes that take place over computer networks, including transmitting child pornography, distributing pirated software, operating fraudulent schemes, and using electronic means to threaten or extort victims;
- Investigate criminals who use computer networks to communicate with each other or to store information;
- Search in criminal investigations of all types for relevant evidence, information, resources, and leads that may be available — and may only be available — online; and
- Use computer networks to communicate with each other and with victims, witnesses, subjects, and members of the general public.

Agents are finding that existing agency guidelines, written for investigations that take place in the physical world, do not answer many of the questions raised by online investigations. For instance, when may law enforcement agents access web pages or enter chat rooms?[2] When should they identify themselves as law enforcement officers in online communications? Do restrictions apply to their personal use of the Internet? When can they communicate electronically with witnesses or suspected criminals? Can they borrow the online identities of cooperating witnesses or impersonate other users? What obligations do agents have to determine

---

[1] This document is not intended to create or confer any rights, privileges, or benefits to prospective or actual witnesses or defendants, nor is it intended to have the force of law or of a directive of the United States Department of Justice or that of any other Department or agency. See United States v. Caceres, 440 U.S. 741 (1979).

[2] Web pages, chat rooms, and other online services are described in **Appendix A, The Online World and Law Enforcement,** Section A, Internet Resources and Services.

whether victims, witnesses, or subjects are operating from abroad? What should they do if they determine that they are investigating in a foreign jurisdiction?

In short, law enforcement agents need to know the rules: under what circumstances may they engage in which online activities? To answer this question, representatives from federal law enforcement agencies came together to form the Online Investigations Working Group (the "Working Group"). The Working Group consisted of over forty members, and included experts from virtually all the federal law enforcement agencies.[3] This document is the product of the Working Group.

It is important to stress that the Working Group's focus is on federal law enforcement agencies that conduct criminal investigations; there is no effort to analyze the issues facing state law enforcement agencies or federal agencies conducting civil, administrative, or counterintelligence investigations. While other agencies may find this document useful, it is intended to apply only to federal law enforcement agents enforcing criminal laws.[4]

---

[3] The components of the Justice Department represented on the Working Group included the Criminal Division (Computer Crime and Intellectual Property Section, Organized Crime and Racketeering Section, Terrorism and Violent Crimes Section, Child Exploitation and Obscenity Section, Office of International Affairs), the Tax Division, the Environment and Natural Resources Division, the Antitrust Division, the Civil Rights Division, the Office of Legal Counsel, the Inspector General's Office, the Attorney General's Advisory Committee, the Executive Office for United States Attorneys, and the Office of Policy Development. All the Justice Department's law enforcement agencies (the Federal Bureau of Investigation, the Drug Enforcement Administration, the Immigration and Naturalization Service, and the United States Marshals Service) were also represented. The Treasury Department sent representatives from the Office of the Undersecretary for Law Enforcement, the Internal Revenue Service, the U.S. Secret Service, the Bureau of Alcohol, Tobacco and Firearms, the U.S. Customs Service, the Federal Law Enforcement Training Center, and the Financial Crimes Enforcement Network (FinCEN). Other law enforcement agencies were also represented, including the Department of Defense, the U.S. Postal Service, the Inspectors General through the President's Council on Integrity and Efficiency, and the Food and Drug Administration. See **Appendix B.**

[4] Although these Principles do not extend to state law enforcement officers (except those conducting joint federal-state investigations), those officers should be aware that online criminal investigations often can raise international concerns, and certain law enforcement techniques

(continued...)

B. The Mission of the Working Group

Once convened, the Working Group set about to identify the issues that online investigations raise, and then to reach consensus on answers that could assist the entire federal law enforcement community. From this process, two central concerns emerged repeatedly:

- How could federal law enforcement agents be given adequate authority to protect public safety online, while fully respecting the important privacy interests of online users?

- How could the many different missions and authorities of federal law enforcement agencies be taken into account, while providing guidance for their common issues arising in online investigations?

With regard to the first concern, the Working Group recognized that law enforcement agents require sufficient leeway to carry out their vital duties in cyberspace. Federal law enforcement agents have a duty to protect the confidentiality, integrity, and availability of data and systems, a responsibility that is uniquely federal because of the national and international character of computer networks. Additionally, these law enforcement agents must protect against the significant harms to the public that can occur when the facilities and resources of computer networks are used for criminal purposes. At a time when criminals are taking greater advantage of online opportunities to further their activities, law enforcement also must be ready to use electronic tools to protect public safety.[5]

At the same time, the Working Group recognized that the excessive presence of law enforcement agents in cyberspace could unduly inhibit speech and association by law-abiding online users, just as it could in the physical world. The Working Group concluded that it is worthwhile to take steps to minimize this inhibiting effect, even in circumstances where neither

---

[4](...continued)
may be governed by treaties that are binding on state as well as federal law enforcement authorities. Accordingly, state law enforcement officers should pay special attention to **Principle 11, International Issues**, and contact the Justice Department's Office of International Affairs (202-514-0000) for guidance when international issues arise.

[5] If agents' online activities were subjected to greater restrictions than their physical-world investigations, criminals would have an incentive to increase their use of online facilities and resources when engaging in illegal conduct.

the Fourth Amendment[6] nor the First Amendment mandates such self-regulation, and the statutory restrictions on obtaining electronic communications (most notably, the Electronic Communications Privacy Act) do not come into play.[7]

The government's voluntary adoption of guidance for agents conducting online investigations should help reassure online users that the law enforcement community will respect civil liberties while protecting users from illegal conduct. As with guidelines governing undercover operations, online investigative guidance reflects the commitment of the federal law enforcement community to balancing the needs of public safety with important competing interests.

With regard to the second basic concern, the Working Group was mindful of the important differences among the many federal law enforcement agencies. Each agency has particular statutes to enforce and a particular scope of authority to carry out its mission. Each operates under a different set of regulations and procedures. As a result, in a given investigative situation in the physical world, an agent from one agency may be permitted to engage in a certain activity while an agent from a different agency might not be allowed to do so absent special permission.

A document that ignored these differences and took a "one size fits all" approach would result in greater consistency across government agencies, in that all agents would have to conduct themselves according to the same rules during online investigations. Such an approach, however, would produce greater inconsistencies within individual agencies, as agents would find

---

[6] Many online resources – from web pages to chat rooms – are available for anyone to use. Because no one can have a reasonable expectation of privacy with respect to information made available to the general public, access to that information by law enforcement does not constitute a Fourth Amendment "search and seizure."

[7] In very general terms, in the absence of a specified exception, the Electronic Communications Privacy Act of 1986 (ECPA) requires law enforcement to obtain a court order to intercept private electronic communications in real time. 18 U.S.C. §§ 2510 et seq. ECPA also generally requires law enforcement to obtain a search warrant to view the contents of unopened e-mail stored by electronic communications providers. 18 U.S.C. §§ 2701 et seq. For a discussion of ECPA, see Federal Guidelines for Searching and Seizing Computers, U.S. Department of Justice, Criminal Division (1994) and Supplement (1999), available online at www.usdoj.gov/criminal/cybercrime.

themselves required to follow a different set of rules depending on whether they happen to be using online or physical world resources to investigate criminal activity. The Working Group concluded that law enforcement agents should be governed by consistent internal agency principles whenever possible, regardless of the medium in which the investigation takes place.

Although a single set of rules that ignores the differences among agencies is not desirable, the Working Group also rejected the notion that each agency should be left to confront these difficult issues independently. Such a course would risk having agencies take wholly divergent approaches to the scope of permissible online activities for reasons unrelated to the differences in their missions. The Working Group concluded that there are significant benefits in taking a common approach to common problems associated with online investigations.

C. The Principles as Analogies

To best address these two core concerns, the Working Group created a document, structured as "Principles" and "Commentary," that operates as a set of analogies between online law enforcement activities and their closest physical-world counterparts. The function of the analogies is simply to translate the less familiar online investigative activities into the kinds of investigative techniques with which agents and agencies are more familiar.[8] These analogies permit each federal agency to apply its own guidelines and procedures to online investigations. Thus, these Principles impose no new restrictions on agents' conduct and, with two very limited exceptions,[9] create no new procedural rules for agents or agencies to follow.

Structuring these Principles as analogies provides law enforcement agents with the same powers, and users with the same protections, as exist in the physical world. For physical world investigations, agency guidelines and practices are carefully structured so that greater evidence of wrongdoing is required to justify using more intrusive law enforcement techniques. For example, a minimally intrusive law enforcement activity, such as accessing publicly available information, can be undertaken based upon relatively little evidence of wrongdoing. By contrast,

---

[8] Appendix A, **The Online World and Law Enforcement,** provides a primer for the types of online services currently available. This Appendix also describes some of the ways criminals use online resources and facilities.

[9] ⌜

b2, b7E

a more intrusive activity, such as an undercover operation, requires a greater showing of wrongdoing and justification for employing the technique.

By fitting online activities into these preexisting policies and practices, the Principles make clear that, in the proper circumstances, law enforcement agents may use the same online resources and facilities as any other users and may engage in the full range of activities online that they may in physical world investigations. However, by insuring that existing agency limits also apply online, the Principles protect the privacy interests of legitimate users in the same way and to the same degree as in the physical world. Similarly, the Principles ensure that the same agency guidelines and policies that govern how law enforcement agents obtain information from foreign sources apply in the online world. See **Principle 11, International Issues.**

Thus, the chief purpose of the Principles is to suggest analogies directing agents to the appropriate policies, practices, and procedures of their agencies. Of course, the differences between the physical world and the online world render many analogies imperfect, and in many places the Principles have had to choose among several plausible alternatives. For example, Internet Relay Chat and similar chat programs share some characteristics with a telephone party line and some with a public meeting. The Working Group selected the public meeting analogy as the one most closely akin, because such online discussions are increasingly serving as a new kind of public meeting not confined by location. See **Principle 3, Real-Time Communications.**

Throughout its analysis, the Working Group drew distinctions in five core areas:

- Whether the proposed law enforcement activity involves collecting information from existing data sources or instead involves communicating with citizens, either openly or on an undercover basis;

- Whether the information that law enforcement agents seek is publicly available (and thus open to anyone who wishes to access it) or is meaningfully restricted (reflecting an intention to keep the information private);

- Whether the information is static (created as a written record with some built-in degree of longevity) or is instead a real-time, transient communication (which typically is not stored and will disappear unless someone makes an effort to preserve it);

- Whether the computer system, data, victim, witness, or subject is domestic (fully within reach of U.S. laws and policies) or located abroad (raising difficult jurisdictional and diplomatic issues); and

- Whether the online activity involves investigating cases or developing leads (when the agencies have a substantial interest in controlling the actions of agents even when nominally off-duty) or instead involves areas (such as general online research) where the government's interest in regulating agents' off-duty conduct is less acute.

Finally, one of the goals of this document is to tie the Principles to concepts that presumably will exist regardless of how the online world evolves, rather than to specific types of online services currently available, an approach which would render them rapidly obsolete. For example, no matter how the World Wide Web evolves, there is likely to always be some set of online services that do not restrict public access. Thus, the analysis in **Principle 1, Obtaining Information From Unrestricted Sources**, will continue to be relevant.

A Note to Prosecutors: In the physical world, agents, rather than prosecutors, generally conduct the bulk of the investigative activity. That activity includes interviewing witnesses, operating undercover, and conducting searches. In online investigations, prosecutors may be tempted to undertake more investigative activity themselves. They may already be familiar with online research, and may reason that, because online investigative work appears to be safe and convenient, there is little risk in visiting the website of a group under investigation or engaging in an online chat with potential witnesses.

Prosecutors should be aware that by investigating online, they may risk being identified by the targets, and, if the case is indicted, may face motions to disqualify on the grounds that they have become a witness. Moreover, the prosecutor may find that he or she has unwittingly interviewed a represented party and potentially violated an ethical restriction, or acted in an undercover capacity in a manner that (if undertaken by an agent) would have required special agency approval. Accordingly, prosecutors are advised to use great care in this area.

PART I: PRINCIPLES GOVERNING OBTAINING INFORMATION

PRINCIPLE 1

OBTAINING INFORMATION FROM UNRESTRICTED SOURCES

Law enforcement agents may obtain information from publicly accessible online sources and facilities under the same conditions as they may obtain information from other sources generally available to the public. This Principle applies to publicly accessible sources located in foreign jurisdictions as well as those in the United States.

COMMENTARY

The Internet and other online facilities allow anyone to offer information to the general public in a form that is rapidly retrievable and searchable from anywhere in the world. As a result, a vast (and burgeoning) quantity of information is available from such sources as the World Wide Web, Usenet newsgroups, electronic mailing lists, and FTP (file transfer protocol) archives.

Naturally, online information on a given topic or about a specific individual or group may be pertinent to a particular law enforcement investigation. To the extent that such material is available to the public,[10] law enforcement should treat it in the same fashion as information available from non-electronic public sources. That is, a law enforcement agent may obtain information from unrestricted sites or sources online in the same circumstances in which the agent could obtain information from other sources generally available to the public, such as newspapers, library research materials, or materials available through a written or oral request.

Obtaining information from online facilities configured for public access is a minimally intrusive law enforcement activity. For Fourth Amendment purposes, an individual does not have a reasonable expectation of privacy in information he or she has made available to the general public (such as a personal "home page" on the web). Similarly, an individual does not

---

[10] Under this Principle, online information available to anyone willing to pay a subscription or other user fee is "available to the public" in the absence of additional access restrictions.

have a reasonable expectation of privacy in personal information that is generally made publicly available by others (such as publicly available Internet telephone directories).

In addition, the rights guaranteed by the First Amendment generally are not implicated when a law enforcement agent obtains publicly available materials. In many cases, the information about an individual contained in databases maintained by others involves neither that person's "speech" nor an exercise of associational rights guaranteed by the First Amendment. Even where materials placed on the Internet represent speech (such as an individual's Web "home page") or expressive association (such as participation in an online newsgroup or mailing list), law enforcement's viewing those materials creates no greater "chill" on the exercise of those rights than does law enforcement's viewing notes or handbills posted on public property.[11]

A. Stored Public Communications

Principle 1 applies not only to relatively static resources such as web pages, but also to other forms of public online interaction that require the communication to be stored electronically. Examples include electronic mail sent to a discussion list, where the message is stored on each addressee's mail server; Usenet, where each posted article is copied to (and stored on) thousands of news servers around the world; and public areas on bulletin board systems (BBSes), where posted articles remain stored on the BBS for viewing at the subscribers' leisure.

When users engaging in public discourse employ these types of communications, they are (or reasonably should be) aware that their communications will be widely available, and that this availability will extend over a significant period of time. Unlike real-time chat sessions (see **Principle 3, Real-Time Communications**), in which the discussions ordinarily are transient, stored communications inherently involve at least some degree of permanence. For instance, Usenet postings commonly persist for a week or more on local news servers (and far longer on archival sites), and mail distributed to an electronic discussion list has a lifetime determined by each subscriber to the list. Under these circumstances, the author of a communication should anticipate that it may be archived or otherwise redistributed to an even wider circle of readers.

---

[11] Note that this principle is intended to apply when the law enforcement activity involves collecting information from existing data sources. Separate principles cover real-time interactive resources such as chat rooms (**Principle 3, Real-Time Communications**) and sites and facilities to which access has been meaningfully limited (**Principle 4, Accessing Restricted Sources**).

It is also worth noting that in most cases involving stored public communications, the author of a posting has no control over who may access that message. Indeed, the author generally will not even know who reads it. On Usenet, for example, the author of a posted article cannot determine which sites (among the tens of thousands of hosts participating in Usenet) will eventually receive his article, let alone ascertain the names of individuals who may read the item. As a result, an investigative agent may access these communications to the same extent as he or she may access other information generally available to the public through non-electronic means.

Note that this Principle is not intended to apply to non-public electronic communications (where access to the public is meaningfully restricted) such as private electronic mail or private chat sessions, communications to which the restrictions imposed by the Electronic Communications Privacy Act of 1986 (ECPA) apply.[12] Cf. 18 U.S.C. § 2511(2)(g)(i) (excluding from ECPA's scope "an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public").

> ***EXAMPLE:*** An agent wishes to read all traffic in the Usenet newsgroup "alt.hackers". Because the articles in the newsgroup are available to the general public, the agent may access those communications if the agent is authorized to obtain similar publicly available information from offline sources such as newsletters.

B. Search Tools

Because of the wealth of available materials and the lack of any consistent topical organization, it is difficult to research publicly accessible information on the Internet without using search tools. Search tools are facilities, resources, or programs that allow a user to find materials pertinent to his or her interests. Search tools operate by requiring the user to define his or her interest by selecting certain words or terms likely to appear in the desired materials (including an individual's name), or by selecting certain topics.

Search tools use automated programs to search through a set of materials (such as websites) and list responsive information. Some search tools operate by "pulling" the list of materials to the user on a one-time basis; others constantly cull the online resources and "push" the materials to the user's computer whenever they find something responsive. Search tools may

---

[12] For a brief discussion of ECPA, see Overview at page 4, footnote 7.

be commercially available to anyone or privately developed for a particular user. There is no doubt that search tools will continue to become more powerful and easier to use.

Generally speaking, law enforcement's use of search tools is beneficial, because it permits law enforcement agents effectively and inexpensively to locate evidence that might be missed in a non-automated search. The use of such tools may also promote privacy: if the search request is tailored appropriately, these tools can filter out irrelevant data from the information to be reviewed by law enforcement personnel. At the same time, however, the effectiveness of search tools arguably increases the degree of intrusiveness because large volumes of information (often covering activity over an extended period of time) can be collected from diverse sources at minimal cost. In light of the increased potential for intrusiveness created by this new technology, agents should be careful not to exceed the legitimate needs of the investigation in crafting online searches.

Comparing a conventional search to an online search for information illustrates the need for carefully tailored online searches. Suppose that during the course of an investigation, the subject mentions an accomplice's name. In a conventional search, the agent is likely to do a criminal history check, search public records, or review the agency's own indices for information about this person. All the information from these searches would be either in the public domain or the product of prior law enforcement activities.

An online search using search tools is apt to generate additional types of material. For example, the accomplice may have a home page, providing his views about a variety of topics. He may have posted communications to mail lists, or be mentioned in the contributions of others. These types of communications may or may not be relevant to the topic of the investigation.

Similar concerns are raised when the search is not for an individual, but for a group. An FBI agent, for example, may wish to search for information relating to particularly violent groups; an IRS agent might seek information on organizations advocating refusal to file tax returns. Such a search may generate information both about the types of organizations that law enforcement may properly investigate, and about those associations and individuals merely exercising their right to free speech. In those circumstances, law enforcement agents should focus solely on the relevant information generated about the appropriate subjects of investigation. See page 14, Section D, The Privacy Act and Other Limitations on Gathering Information.

One important investigative issue needs to be emphasized. It is possible for the administrators of websites or commercially available search tools to track searches by or about a

particular user or group of users. A program could be written, for instance, to enable the administrators to track and store all visits or searches conducted from an online address ending in "fbi.gov". Thus, an agent visiting a website or using a search tool to investigate a certain individual may inadvertently compromise the confidentiality of the investigation. Accordingly, agents may need to use a "non-identifying" online address (or use similar measures, such as an anonymous re-mailer) to obtain information online.

> ***EXAMPLE***: A law enforcement agency is investigating allegations that an individual is defrauding consumers by advertising and selling a device he claims will cure various forms of serious diseases. The law enforcement agents may use search tools to obtain publicly available electronic information for any investigative purpose for which they could have obtained publicly available information accessible through traditional means. This information may include research that demonstrates the device to be effective or ineffective, advertising materials for the device contained in publicly available databases or in the subject's web home page, background information on the target, or any other information relevant to the investigation.

C. International Issues and Publicly Available Materials

Principle 1 is intended to pertain both to materials found in servers located within the U.S. and to any publicly available resource located outside the U.S. This is true whether the resource provides information (such as a web site), provides a means for communications (such as a mailing list hosted through a foreign computer), or otherwise can be accessed through any online service provider. Accordingly, agents need not take any special steps to discover the physical location of the publicly available resource, nor do they need to follow any special procedures before accessing and downloading the information, even if they happen to know the facility is in a foreign jurisdiction.

Several factors support this conclusion. First, accessing such publicly available material is minimally intrusive. Persons or organizations who make information available in this manner may be deemed to have voluntarily disclosed it to the world. Moreover, foreign governments are (or should be) aware that law enforcement agents in the U.S. and other countries make use of public online resources in their investigations. Indeed, there is a growing international consensus

that law enforcement access to publicly available online materials raises no significant sovereignty issues.[13]

In addition, purely practical considerations militate against imposing limitations on access to publicly accessible materials located on foreign computers. Often, a domestic resource on the Internet may be linked to information contained on a computer located in a foreign jurisdiction. It may be extremely difficult or even impossible to determine where the linked information is located before it is accessed. Additionally, an agent using a search tool may unwittingly cause information to be downloaded from a foreign site to a domestic computer. Agents should not be obligated to follow a completely different set of rules depending on the location of the source computer so long as they are gathering publicly available information.

This reasoning does not extend, however, to overseas resources that are not configured for public access. Agents should be aware that their use of such resources, or their initiation of personal contact with residents of a foreign state, may violate foreign law. In addition, activity by U.S. law enforcement in such areas may be regarded as a violation of the other nation's sovereignty, creating the potential for serious diplomatic conflict. A separate principle, **Principle 11, International Issues,** addresses the important issues raised by accessing nonpublic foreign resources.

> *EXAMPLE:* Law enforcement agents are investigating an officer of an offshore bank suspected of participating in an international money laundering operation. Assuming the agency would permit its agents to access publicly available material at U.S. sites, the

---

[13] See Principle 9, Statement of Principles, Principles and Action Plan to Combat High-Tech Crime, Meeting of Justice and Interior Ministers of the Eight, December 9-10, 1997 (available on the Computer Crime and Intellectual Property Section's web page, www.usdoj.gov/criminal/cybercrime):

"Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides."

Although many countries support this approach, some countries may still object to a foreign law enforcement agent's accessing information from a publicly available site. Such objections may need to be addressed in individual instances, but should not affect the publicly stated position of the United States that access to such sites does not raise transborder issues.

agents may obtain information about the officer from a foreign website or other foreign facility if it is configured for public access.

D. The Privacy Act and Other Limitations on Gathering Information

Although collecting information from unrestricted sites is minimally intrusive, agents must remain aware of statutes and internal agency guidelines that may limit when they can collect or maintain records of such information, even if such information appears in public, unrestricted sources.

The principal statute in this area is the Privacy Act. The Privacy Act provides that an agency that maintains a system of records shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7). The Act further defines the term "maintain" to include "maintain, collect, use or disseminate." § 552a(a)(3). Accordingly, unless one of the exceptions within subsection (e)(7) is met, an agent may not "maintain, collect, use or disseminate" any record "describing how any individual exercises rights guaranteed by the First Amendment." The First Amendment protects, to one degree or another, much — although not all — of an individual's public activities on the Internet, such as the publication or dissemination of information or opinion.

The Privacy Act's (e)(7) provision applies only to individuals. "Individuals," in turn, is defined to mean citizens of the United States or aliens lawfully admitted for permanent residence. 5 U.S.C. § 552a(a)(2). The Act imposes no restriction on the maintenance of records reflecting expressive activities engaged in solely by foreign persons, or by organizations, rather than individuals.

Notably, the Privacy Act does not prohibit an agency from investigating or observing an individual's First Amendment activities, but does impose a restriction on the creation, maintenance and use of records — such as hard copies, print-outs or notes — describing such activities. Such records may, however, be created and maintained if they are "pertinent to and within the scope of an authorized law enforcement activity." This means that the records of an

individual's exercise of First Amendment rights may be created and maintained if they would be relevant to an authorized law enforcement activity.[14]

The Privacy Act itself does not define the circumstances under which law enforcement activities are "authorized." Each agency has its own standards and procedures that regulate when agents may initiate an inquiry or investigation, and agents should look to those procedures and standards in order to determine what constitutes the scope of its agency's "authorized law enforcement activities" for purposes of the Privacy Act.

Just as there are circumstances when an agency may not maintain records, there are some circumstances when it should. Agency policies regarding recordkeeping also apply to online investigations. Agents must keep track of what they are doing during an investigation, whether it takes place in the physical world or online. Such recordkeeping promotes an efficient and effective investigation, serves internal administrative needs, and provides evidence to rebut any subsequent suggestion that the agent acted improperly in an investigation.

The need to keep track of an investigation must, of course, be balanced with considerations against keeping voluminous irrelevant records. Even carefully tailored online searches are likely to generate irrelevant material that agency record-keeping policies may permit to be discarded. An agent should consider reasonable methods to balance these competing concerns, such as logging or otherwise preserving a record of the searches employed and the pertinent results.

---

[14] See Patterson v. FBI, 893 F.2d 595, 603 (3d Cir. 1990); Jabara v. Webster, 691 F.2d 272, 279 (6th Cir. 1982). Other courts have adopted slightly different, more restrictive, tests for determining when record collection is "pertinent" to authorized activities. See Clarkson v. IRS, 678 F.2d 1368, 1375 (11th Cir. 1982); MacPherson v. IRS, 803 F.2d 479, 484-85 & n.9 (9th Cir. 1986). In those circuits, "relevance" to an authorized activity, standing alone, might not always be sufficient to justify recordkeeping of First Amendment activities. Consultation with agency general counsel in this area is advised.