ONLINE INVESTIGATIVE PRINCIPLES FOR FEDERAL LAW ENFORCEMENT AGENTS

PREPARED BY:

THE ONLINE INVESTIGATIONS
WORKING GROUP

Final Version (November 1999)

TABLE OF CONTENTS

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
ONLINE UNDERCOVER FACILITIES

Just as law enforcement agencies may establish physical-world undercover entities, they also may establish online undercover facilities, such as bulletin board systems, Internet service providers, and World Wide Web sites, which covertly offer information or services to the public. Online undercover facilities, however, can raise novel and complex legal issues, especially if law enforcement agents seek to use the system administrator's powers for criminal investigative purposes. Further, these facilities may raise unique and sensitive policy issues involving privacy, international sovereignty, and unintended harm to unknown third parties.

Because of these concerns, a proposed online undercover facility, like any undercover entity, may be established only if the operation is authorized pursuant to the agency's guidelines and procedures for evaluating undercover operations. In addition, unless the proposed online undercover facility would merely provide information to members of the public or accounts to law enforcement agents, the agency or federal prosecutor involved in the investigation must consult in advance with the "Computer and Telecommunications Coordinator" (CTC) in the United States Attorney's office in the district in which the operation will be based or with the Computer Crime and Intellectual Property Section (CCIPS) of the Justice Department's Criminal Division. An attorney from the Section can be reached at (202) 514-1026 or through the Justice Command Center at (202) 514-5000.

Agencies that already consult with the Justice Department as part of their internal review process for undercover operations may comply with this requirement by providing an extra copy of the undercover proposal to the CTC or to CCIPS, as appropriate.

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
APPROPRIATING ONLINE IDENTITY

"Appropriating online identity" occurs when a law enforcement agent electronically communicates with others by deliberately assuming the known online identity (such as the username) 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. To appropriate online identity, a law enforcement agent or a federal prosecutor involved in the investigation must obtain the concurrence of the United States Attorney's Office's "Computer and Telecommunications Coordinator" (CTC) or the Computer Crime and Intellectual Property Section. An attorney from the Section can be reached at (202) 514-1026 or through the Justice Command Center at (202) 514-5000. In rare instances, it will be necessary for law enforcement agents to appropriate online identity immediately in order to take advantage of a perishable opportunity to investigate serious criminal activity. In those circumstances, they may appropriate identity and notify the Computer Crime and Intellectual Property Section within 48 hours thereafter.

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.

[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).

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 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.

---

[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.

[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**.

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]

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?

[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 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.

- 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]

[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.

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 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

---

[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.

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

---

[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] See **Principle 7, Online Undercover Facilities** (creating consultation requirement) and **Principle 9, Appropriating Online Identity** (creating concurrence requirement).

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.

[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.

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 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.

[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**).

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.

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

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

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 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

[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.

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 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

---

[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.

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.

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.

COMMENTARY

An essential feature of public computer networks is the public nature of certain identifying information such as domain names (e.g., usdoj.gov), Internet Protocol (IP) addresses (e.g.,127.0.0.1), and similar data. Such information is inherently open to view in the network's current configuration. A separate category of information — relating to specific users on individual systems — need not be openly available, although in practice many Internet sites make this information accessible to system users or even to outsiders. For both categories of information, several common software tools exist for retrieving the data locally or from remote sites.

The first general category of tools provides data about host computers or networks. This group of tools includes computer commands that indicate whether a site is currently connected to a network; the path over a network between two host computers; the names of host computers on a sub-network; or other information about a host computer's relationship to its closest neighbors. The information revealed by these commands is essential to the interactions between sites on a computer network, and as such is generally available throughout the network. An agent may seek this information for any legitimate investigative purpose.

The second category of tools — those for obtaining information about individual users — may reveal the real name associated with a username; the time and date the user last logged in; the specific activity of a user who is currently logged into a system; or even a user's postal address or telephone number. The extent to which this information is openly available, either to other users on a given system or to anyone on the network at large, is controlled by the user

and/or the user's system administrator. In many cases, a system operator may disable or curtail the information reported by the relevant software commands, and users often have the ability to decide what information to make available about themselves.

Thus, user information available through conventional information tools (such as the "finger" command in the Unix operating system) is essentially analogous to a person's telephone number. Users know or should know that identifying information about them may be available on their sites, just as customers are on notice that their telephone numbers and addresses are obtainable from telephone directories unless they take steps to withhold that information.

Agents must be alert to the possibility that the user information they obtain from lookup commands may be erroneous or deliberately false. The reliability of this information will depend on the nature of the command used and on the degree to which the host system allows a user to control the information displayed.

Finally, agents must be careful to use these information-gathering tools only as conventionally permitted and not in a manner unauthorized by the system (as by exploiting design flaws in the program to circumvent operating system protections). Likewise, this Principle does not permit the use of tools commonly available on the Internet (such as "sniffer" programs which can be used to intercept the usernames and passwords of authorized users) if their use would violate statutory restrictions (such as the Electronic Communications Privacy Act). The critical test is the degree of authorization granted by the system to all users in the agent's class.

As with **Principle 1**, **Obtaining Information from Unrestricted Sources**, this Principle applies not only to materials located within the U.S., but also to any publicly available resource stored on computers located in another country. This rule does not extend, however, to overseas resources not configured for public access. A separate principle, **Principle 11**, **International Issues,** addresses the serious issues raised by accessing nonpublic foreign resources.

> ***EXAMPLE:*** An agent conducting an online investigation has reason to believe that the user with username "RobtFrost" has information pertinent to the investigation. If agency guidelines would allow the agent to look up a potential witness's phone number or address under similar circumstances, the agent may use conventional system commands to

acquire the information about “RobtFrost” (such as a user profile) publicly available on the computer system.

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.

COMMENTARY

Facilities such as Internet Relay Chat (IRC), and its analogues within individual service providers (such as "chat rooms"), permit online users to engage in real-time discussions. Participants can normally make these discussions private — i.e., prevent access by the general public — in which case the protections and requirements of the Electronic Communications Privacy Act (ECPA) apply.[15] Principle 3 is directed only at those online discussions to which public access has not been restricted; in such cases, ECPA affords no statutory protection to the communications (see 18 U.S.C. § 2511(2)(g)), and the absence of any reasonable expectation of privacy means that law enforcement's observing or recording of such communications would not violate the Fourth Amendment. Further, Principle 3 involves only agents passively observing the discussion. When an agent's activity in a real-time forum crosses from mere monitoring into active participation, it raises issues discussed in **Part II** of these Principles, **Principles Governing Communications Online**.

Public chat rooms, IRC channels, and similar sites are most analogous to public meetings in physical space. Attendance may be unrestricted, and the purpose is to exchange ideas and information. To be sure, chat rooms share these characteristics with some sites that store electronic communications, such as newsgroups and mailing lists, addressed in **Principle 1**, **Obtaining Information from Unrestricted Sources**. In chat rooms, however, the discussion takes place in real time, and the underlying method of distributing chat room communications does not require storage. These features create an environment that encourages the immediacy and spontaneity typical of an in-person dialogue, even though participants know that they or others can create a transcript of their discussions by turning on their computer's logging function.

---

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

Different law enforcement agencies have different internal guidelines governing when agents may observe public meetings. Some of those restrictions on agents' attendance are meant to ensure that members of the public feel free to associate knowing that law enforcement agents will only be observing if there is a sufficient reason for their presence. These restrictions apply equally to meetings taking place in physical space and online. Indeed, as people use online communications to replace physical-world meetings, law enforcement agencies should treat them with equal respect.

Some of the restrictions on attending physical-world meetings, however, may not apply to the online environment. In the physical world, agencies must be concerned that an agent appearing in person may be recognized; that fact, in turn, may cause other participants to believe, rightly or wrongly, that they are under investigation, or it may lead them to conclude that the agent (and possibly the agency) agrees with their views. Although many online chat facilities allow participants to know who else is present in the forum, the available information (often only a user-selected nickname) generally does not reveal a participant's real-world identity.[16] In determining whether to permit an agent to attend a public meeting online, the agency must recognize that these important differences may support allowing an agent to observe an online meeting where the agency would be reluctant to allow the agent to appear if a physical-world meeting were held on the same topic.

Some agencies' internal guidelines may impose additional limits on when agents attending public meetings may record what they hear. Principle 3 does not propose that these same limits apply to agents logging (recording) real-time public electronic communications to preserve a transcript of the communications. Because chat software commonly includes an automatic logging function, chat room participants are less justified than public meeting attendees in believing that their words will not be recorded. If an agency believes it appropriate to establish

[16] Whether a particular facility allows participants in the chat room to see the online identity of other participants should not be relevant to when law enforcement may passively observe and log the discussion.

additional limits on an agent's ability to record exchanges in chat rooms, it should adopt explicit rules to that effect.

Note that when an agency maintains a record of the activity in a chat room, the Privacy Act comes into play. Because chat rooms should be treated like public meetings, the "authorized law enforcement activity" provision of the Privacy Act should apply. (See the discussion of Privacy Act subsection (e)(7) in the Commentary to **Principle 1, Obtaining Information from Unrestricted Sources**.) Additionally, real-time communications can involve participants from other countries. Foreign countries may object to United States agents both attending and recording from chat rooms either located in a foreign country or in which a foreign national participates. These concerns are further addressed in **Principle 11, International Issues**.

***EXAMPLE*:** An agent wishes to monitor, but not actively participate in, an IRC channel discussion about methods for manufacturing explosive materials. The agent may monitor the discussion if he or she would be permitted to attend a public meeting devoted to the same topic. The agent may also create an automated running transcript of the discussion unless agency guidelines impose additional restrictions.

PRINCIPLE 4

ACCESSING RESTRICTED SOURCES

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

COMMENTARY

In the online world, as in the physical world, some individuals, resources, or facilities may choose not to make their information or services available to all, but instead may place restrictions on who may access their services. Some may open their sites only to persons of a particular political, religious, geographical, or interest group. Others may decide to open their facilities to everyone except law enforcement personnel.

Online technology permits such restrictions. For example, sites and services can be protected by passwords, allowing only persons authorized by the system operator to access them. Similarly, most real-time "chat" programs also permit private conversations that are not open to the general public. Even sites that are otherwise open to the public may attempt to exclude law enforcement through either passive measures (such a banner saying "police not welcome") or active measures (such as requiring a negative response to the question "Are you a police officer?" before allowing access).

When individuals carve out private places in the online world, law enforcement must respect those restrictions to the extent they create recognizable expectations of privacy. Law enforcement may access such places only if they have authority to enter similarly restricted places in the physical world. The Fourth Amendment allows law enforcement agents to access

private places only when they have consent of the owner or user, a warrant authorizing them to enter, or a legally recognized exception to the warrant requirement.[17]

[17] In addition, the Electronic Communications Privacy Act (ECPA) protects the individual's right to privacy in the contents of qualifying electronic communications to an even greater extent than does the Fourth Amendment. For a brief discussion of ECPA, see Overview at page 4, footnote 7.

In the physical world, it has long been settled that the Fourth Amendment's protection of an individual's "reasonable expectation of privacy" does not extend to areas a person knowingly opens to public access. Similarly, measures that do not functionally bar the public from entry into a place or that permit public view of a place generally have been held ineffective to create an expectation of privacy.[18] Thus, a website banner inviting all but law enforcement agents to use a system is highly unlikely to be considered sufficient to create a reasonable expectation of privacy.

Even where access is sufficiently limited to create a reasonable expectation of privacy in the online site, law enforcement agents conducting investigations may enter non-public premises with the consent of a person who is authorized to grant it.[19] That consent is not vitiated even if

[18] For example, "no trespassing" signs that do not functionally bar public entry or preclude public view have generally been held ineffective to create a reasonable expectation of privacy, and police may enter or look around such areas that are in plain view. See Oliver v. United States, 466 U.S. 170 (1984).

[19] Valid consent to enter a restricted area of an online facility may be obtained from any individual who has the authority, or appears to have the authority, to permit others to enter. The system operator or system administrator, by virtue of his or her "superuser" status, has the technical ability to permit access to anyone, much like a landlord may have a key to every apartment in a building. Like the landlord, however, the system administrator's technical capability is not the equivalent of legal authority to permit law enforcement to enter the system or to access every part of the system. Other factors (including applicable statutes) must be considered in determining whether the system operator is one of the persons who may give a valid consent to enter the specific areas law enforcement seeks to access.

it was based on a false self-identification by the law enforcement agent. Thus, if they are following their agency's rules, law enforcement agents may use undercover identities to obtain access to restricted facilities, whether in physical space or online. See Hoffa v. United States, 385 U.S. 293 (1966); **Principle 6, Undercover Communications**. A misrepresentation made in order to gain access to an online facility will be governed by the law enforcement agency's rules on undercover contacts; overt contacts or undercover contacts, with or without misrepresentation, reaching internationally into restricted sources will invoke agency rules relating to extraterritorial activities and extraterritorial undercover contacts. See **Principle 11, International Issues**.

As in the physical world, agents passing without permission beyond a "keep out" sign or banner in the online world must restrict their activities to those allowed to the general public. The implied invitation of public access does not extend to non-public areas of the facility (such as password-protected directories or other areas of the computer system not intended for public access). It also does not permit agents to engage in any activity not permitted to other members of the public. Similarly, consent to enter a facility or to examine or obtain information from one part of a system does not permit the agent to access other parts of the system to which consent to enter has not been provided.

> ***EXAMPLE:*** A business under investigation for fraud operates a computer bulletin board system (BBS) through which members of the public can obtain information about the business and place orders. An agent conducting an investigation of the alleged fraud dials the BBS and discovers on the initial screen a banner that says "Police Not Welcome." The agent may ignore the banner and enter the BBS under the same rules that permit him or her to enter places open to the public in the physical world.
>
> Once on the BBS, the agent views a menu that has three choices. Option one provides the user with information about the business. The second choice says "Press here to enter and to certify that you are not a law enforcement officer." The third option allows entry to an area reserved for employees and requires a password to enter.
>
> The agent may select choice one, and consider the information presented to him to be in plain view. By selecting option two, the agent is affirmatively misrepresenting his identity, and may make that selection if his agency's undercover procedures permit. The third area is a non-public area of the BBS, and the agent may only enter that area with permission from an official of the BBS authorized to grant entry, a search warrant, or

other legal authority, just as he may not enter uninvited into an office marked “private” in a place of business. If the agent is given consent by an employee of the system, the agent may enter that area and view whatever contents are in plain view or are within the terms of the consent.

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 devices, 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.

COMMENTARY

A. Online Communications While on Duty

One of the most important functions computers perform is helping people communicate with each other. Electronic communications can take many forms, including not only e-mail (the most widely used form) but also Usenet newsgroups and Internet Relay Chat.

Communicating electronically offers certain significant advantages over communicating face-to-face or on the telephone. First, online communications permit the transfer of more information because files (containing text, voice, graphics, or a combination thereof) can be included in a communication. Second, many forms of electronic communication, such as e-mail or Usenet newsgroups, do not require the parties to be available at the same time. Third, electronic communications can be sent to many people simultaneously.

Law enforcement is no less entitled than any other sector of society to communicate online. Indeed, law enforcement must be able to employ a full array of communication tools in order to perform its job effectively. Accordingly, just as law enforcement agents may need a telephone for official communications, they may need e-mail to communicate with other members of the law enforcement community and with crime victims, informants, witnesses, members of the general public, and even targets of investigations. (In communicating through computers, agents must, of course, be extremely careful about securing sensitive material and must strictly follow their agency's prescribed procedures for transmitting classified information.)

Generally, agency rules governing in-person or telephonic communications by agents should apply to online communications. For example, the rules of conduct governing agents' communications with witnesses, including whether agents need to disclose their affiliation with law enforcement, should apply whether the communication is taking place in person, over the telephone, or online. See **Principle 6, Undercover Communications**. Similarly, if an agent is permitted to use the telephone to speak to a witness, informant, victim, or fellow agent, there is no reason (assuming adequate security measures are in place) that such communication cannot take place through the computer.

Of course, special sensitivities apply in international electronic communications by law enforcement agents, particularly when those communications are to crime victims, informants, witnesses, members of the general public, or targets of investigations. Some countries may bar these communications and criminally penalize those who attempt to make them. As a general rule, however, communicating internationally through electronic means should be governed by the same rules and policies as international communications using other means. That is, if an agent is authorized to use the telephone to call her counterpart in a foreign nation, she may use her computer to accomplish the same purpose.[20] Similarly, if a country bars direct telephone calls to witnesses or informants, the online communication would be barred also. These same considerations apply to the preservation or recording of communications, discussed below. See **Principle 11, International Issues**.

B. Preserving Records of Communications

Some methods of communication, such as e-mail, inherently create an electronic record which will persist until it is deleted by the user or by the system. Agents should retain the contents of such communications if they would have kept the message had it been written on paper. The method of preserving such communications — electronic storage or hard-copy printout (including transmission information) — may be governed by agency or government-wide procedures for the preservation of electronic communications. Agency regulations, the

[20] Some agencies may permit certain international communications to be carried out through letters but not through telephone calls. As long as the letter receives the necessary internal approvals, it should make no difference whether a physical copy is sent through the mails or an electronic copy is e-mailed or faxed.

Freedom of Information Act, or other statutes may also affect the decision whether to preserve an electronic message, even if the message would not have been preserved had it been written on paper.

Other types of communications, however, do not automatically create an electronic record. Real-time communications, such as IRC, are not automatically stored by the system, but may be recorded (via a computer logging function) by one or more of the participants. Recording real time communications that are open to the public is discussed in **Principle 3, Real-time Communications**. Agencies should apply its policies on recording analogous face-to-face or telephonic conversations when an agent is considering whether to record a real time private electronic conversation in which the agent is a participant. See **Principle 6, Undercover Communications**.

> ***EXAMPLE 1***: A law enforcement agent wants to contact a person he has observed in a chat room to determine if that person has knowledge about a crime the agent is investigating. The agent may communicate with the potential witness through electronic means if authorized to communicate with the witness over the telephone or in person. If the agent and the witness communicate electronically, the agent may record the discussion, with consent or surreptitiously, if the agent has the authorization required to record the conversation over the telephone.

> ***EXAMPLE 2:*** The agent in Example 1 interviews the witness electronically, writes a report of that interview, and needs to share that report with a law enforcement officer from another agency who is also working on the investigation. Using appropriate safeguards to preserve information security, the agent may send the report electronically if he could send it through the mail. The electronic communication (including transmission information) between the agents should be preserved, in accordance with agency procedures for the preservation of electronic communications, if a copy of the communication would have been kept had it been written on paper.

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.

COMMENTARY

A. Disclosing Affiliation with Law Enforcement in Online Communications

Agency guidelines and procedures generally require agents to disclose that they are affiliated with law enforcement at the outset of interviews or other investigative conversations. There are, however, circumstances in which agency guidelines and procedures do not oblige agents to disclose that they are affiliated with law enforcement when communicating in person or over the telephone. These circumstances may include incidental communications, such as asking directions, where the agent's connection to law enforcement is irrelevant to the communication. More significantly, under certain circumstances, agency guidelines permit agents to act in an "undercover" capacity and operate under an assumed name or fictitious identity. The undercover technique is central to law enforcement's ability to infiltrate sophisticated and dangerous criminal organizations, both to gather necessary intelligence on their activities and to accumulate evidence for use at trial.

It can be argued that, because of the differences between physical-world and online communications, agents should not be obligated to disclose their affiliation with law enforcement online as they would in the physical world. In the physical world, most people, including law enforcement agents, normally identify themselves accurately unless there is an important reason why they should not. In the online world, by contrast, different conventions and expectations often apply: people communicate through usernames, which are often self-selected, changeable, and may bear no relationship to the true identity of the user. If online users are free to operate

under any username, should agents likewise be free to communicate without disclosing their true identities?

These Principles reject that approach, which would foster inconsistency between the rules governing physical world and online investigations. Unless the agent is authorized to be acting undercover, witnesses should know, regardless of the medium in which the conversation is taking place, that a law enforcement officer is conducting a duly authorized investigation when seeking information from them. Disclosing affiliation with law enforcement allows the witness to understand the significance of responding truthfully and completely.

Thus, agents are required to affirmatively disclose their status as law enforcement officers when communicating online just as they would (usually by displaying credentials) in physical world communications.[21] That requirement applies whether the agent is using his real name and

[21] Agents attempting to obtain information from Internet service providers must disclose their affiliations with government (whether communicating electronically or otherwise) if the information they seek is covered by the provisions of the Electronic Communications Privacy Act (ECPA). There are some provisions of ECPA that prohibit service providers from disclosing certain information if the recipient is a governmental entity. For example, a service provider may disclose records pertaining to a customer or subscriber to any person other than a government entity without limitation. 18 U.S.C. § 2703(c)(1)(A). By contrast, an electronic service provider may disclose such records to a government entity only with the consent of the customer or

government address (johnsmith@usdoj.gov), his real name and a non-identifying address (johnsmith@any-isp.com) or a non-identifying name and address (11223@any-isp.com). The issue here is not whether the online address is false or misleading; rather, it is whether the disclosure adequately informs the other party to the communication that he or she is talking to a law enforcement officer.[22]

---

subscriber or through certain types of compulsory process. 18 U.S.C. § 2703(c)(1)(B). Although it may not be required by ECPA, as a matter of policy, agents should disclose their affiliations with government before asking for information covered by this statute. See Supplement to Federal Guidelines for Searching and Seizing Computers, U.S. Department of Justice, Criminal Division (1999), available at www.usdoj.gov/criminal/cybercrime.

[22] There may be times when a username or domain name sufficiently identifies a law enforcement agent. But given the relatively uncontrolled manner in which user and domain names are selected and assigned, law enforcement agents should usually state their law enforcement affiliations affirmatively at the outset of the online communication, regardless of online address, particularly when they communicate with an individual for the first time.

Applying the same rules for disclosing law enforcement affiliation in the online and physical worlds will not unduly hinder legitimate law enforcement activities, for three reasons. First, the rule only applies to two-way communications. As noted in **Part I, Principles Governing Obtaining Information**, agents may obtain information from publicly available sources by using either identifying or non-identifying online addresses. Certain exchanges of information required to obtain access to such sites (such as automated registration in which the affiliation of the registrant is irrelevant to whether permission to access the site will be granted) may be so insignificant as to not obligate agents to disclose their affiliation with law enforcement. It is generally only when agents communicate actively with subjects or witnesses — usually to seek evidence of a crime — that the obligation to self-identify (or, alternatively, to be authorized to engage in communications without accurate self-identification) applies.

Second, most agency rules permit, absent unusually sensitive circumstances, certain kinds of isolated communications to take place without disclosing law enforcement affiliation or seeking approval for a full-scale undercover operation. These rules permit agents, for example, to make pretext calls or other preliminary contacts without going through an elaborate approval process. Applying these same rules online will provide agents with the flexibility necessary to carry out their duties.

Finally, agents can, where appropriate, seek authorization to conduct undercover operations online, just as they would in conducting physical-world investigations.

One more point bears noting here. Just as agents normally should identify themselves when communicating officially, they should take care when communicating in a personal capacity from online addresses that identify them as law enforcement. The question whether an agent may use an agency online address for personal or unofficial communications is usually determined by the particular agency's regulations on use of official property. Any such use will also be governed by the Office of Government Ethics' Standards of Conduct for Government Employees, as well as by supplemental agency regulation. For example, issues may arise regarding the extent to which personal opinions or beliefs expressed from an official e-mail address may be taken by outsiders to be those of the agency itself, much as if the communication were written on official agency stationery. See **Principle 10, Online Activity By Agents During Personal Time.**

B. Online Undercover Activities Authorized

Just as the rules obligating agents to disclose their affiliations with law enforcement carry over into the online world, so should the rules permitting them to operate undercover. The undercover technique is as valuable to combat crime in the online world as it is in the physical world. Often, only through online undercover techniques can law enforcement infiltrate groups of online child pornographers, hackers, and other criminal organizations and associations. (See **Appendix A, The Online World and Law Enforcement**, at A-5 to A-9.) Moreover, other criminal organizations, such as traditional organized crime groups, are increasingly using online facilities to communicate and to conduct their criminal enterprises. The law enforcement techniques that have been used to combat such organizations, including undercover operations, must therefore be adapted to cyberspace.[23]

Although the undercover technique is an effective weapon against crime, it can also be intrusive, deceptive, and may even require law enforcement agents to gain the criminal's trust by appearing to engage in illegal acts. Thus, law enforcement agencies require proposed undercover operations to undergo a review process in which all the benefits and risks of the proposed operation are carefully assessed and evaluated.

---

[23] Undercover communications with individuals located in foreign countries are likely to have serious international repercussions. Most foreign countries will protest the use of undercover techniques with their citizens on their soil, particularly if law enforcement agents in that country are not permitted to communicate undercover. Further, foreign law enforcement may unknowingly investigate U.S. undercover agents believing them to be part of a criminal group. Because all this could seriously disrupt our law enforcement and diplomatic relationships, it is essential to obtain the appropriate clearances before such communications are undertaken. See, **Principle 11, International Issues**.

The guidelines and procedures employed by the agencies to evaluate and monitor undercover operations should govern equally well in the online context. An agent who is considering an online undercover operation should consult the agency's guidelines and seek the necessary approvals. An official deciding whether to approve or disapprove such an operation should weigh the risks and benefits of the proposed operation and make the determination based on an evaluation of the pertinent factors, just as if the proposed activity were taking place in physical space.[24]

C. Defining an Undercover Online Contact

As noted above, absent especially sensitive circumstances, most agencies permit some small number of undercover communications, sometimes called "contacts," without formal review or approval. This gives agents the authority to make isolated pretext calls, while ensuring that long-term undercover activities are given the careful scrutiny they deserve.

The nature of online communications makes counting undercover "contacts" much more difficult than in the physical world. Generally, a physical-world contact consists of a single communication or conversation, either face-to-face or over the telephone, naturally circumscribed in time.

Communicating in cyberspace is different. Consider the following scenario: A subject proposes to an agent operating undercover that they might commit a crime together. The agent responds by e-mail, asking for more details. The subject provides more details, and asks for the

[24] Special considerations are involved in creating certain kinds of online undercover communication facilities as part of an undercover operation, such as interactive web sites covertly run by law enforcement. These considerations are addressed in **Principle 7**, **Online Undercover Facilities**.

names of mutual acquaintances who will vouch for the agent. When the agent provides these names, the subject agrees to a meeting. For purposes of the undercover guidelines, is this one undercover contact, five undercover contacts, or somewhere in between?

Two basic approaches could be taken to address this difficult issue: (i) a formalistic, hard and fast rule; or (ii) a practical standard that treats electronic "contacts" more like physical-world conversations, at some cost to simplicity. The Principles take the second approach.

Of course, it would be easy to consider any transmission from an agent, regardless of its brevity or content, as a separate undercover contact. That rule would be easy to follow, but counting contacts in that fashion would trigger the undercover approval process much more often when communicating online than when communicating over the telephone or face-to-face. Alternatively, the undercover contact could be limited by time or event: that is, any communications that take place in a certain period (e.g., a single day or a single log-in session) with a particular party could be regarded as a single contact, regardless of the number of separate transmissions. Such a rule, however, would generate inconsistency by allowing a single contact to consist of an indefinite number of transmissions, without regard to the content of those transmissions.

Rather than adopting an approach that creates a divergence between online and physical world methods of counting contacts, the Principles direct agents to count a discrete conversation as one contact, just as they would an in-person conversation. Agents may apply a variety of factors in deciding how to group separate transmissions into a single conversation.

First, the agent should consider the amount of time between strands of the conversation. For instance, if the transmissions are fired back and forth within the space of an hour, they are more likely to constitute a single, discrete conversation than if they are strung out over a matter of weeks.

Second, the agent should consider the number of transmissions. A transmission, a response, and a reply to that response are more likely to be grouped as a single contact than a series of ten exchanges back and forth.

Third, the agent should consider the number of interruptions and topical transitions. In the scenario set forth above, for example, if the bulk of the communications take place in a short time, but a considerable delay ensues after the agent provides the subject with his "references," it

is fair to end the first contact with the agent's providing the references and begin the second with the subject's response.

Fourth, the agent should consider the medium in which the communications are exchanged. Conversations in chat rooms, for example, are "real-time." Because participants all converse at the same time, rather than leaving messages for one another, these chat sessions have a more easily defined beginning, middle, and end than do communications taking place over e-mail. Thus, a single chat room session should generally be considered a single contact, even if the conversation is lengthy and involves more than one topic.

Finally, the agent should always remember the purpose of the rule. If the agent is anticipating that the online undercover communication will not be an isolated event, but will lead to a series of contacts that would require agency approval if undertaken in the physical world, he or she should resolve any doubts by seeking the necessary undercover approvals in advance.

> ***EXAMPLE 1:*** A law enforcement agent wishes to communicate with a potential witness online. He does not have authority under his agency's guidelines to engage in undercover communications and, if the communication were to occur in person, he would identify himself to the witness as a law enforcement officer. The agent should accurately identify himself in the online communication. Even if the agent's e-mail address suggests his affiliation with law enforcement, the agent should affirmatively inform the witness in their initial online communication that he is a law enforcement agent.
>
> ***EXAMPLE 2:*** An agent is seeking information about an attack on a computer system. She proposes to inquire about the attack, without disclosing her affiliation with law enforcement, in a chat room frequented by the suspected computer hackers. If the agency would consider such a communication to be an undercover contact had it occurred in person or over the telephone, it should be considered an undercover contact online, subject to the same procedures and constraints.
>
> ***EXAMPLE 3:*** The agent in Example 2 is permitted by her agency guidelines to make the isolated inquiry without seeking approval for an undercover operation. One of the participants in the chat room states that he has information, and a conversation ensues. The agent and the participant each send one message containing ten lines of text about the incident. The participant later follows up with an e-mail, and the agent responds immediately after reading the message. The agent should consider, for the purposes of the

agency's undercover guidelines, that the first conversation in the chat room is a single contact because it is limited in time, place, number of transmissions, and topic. The e-mail exchange should be considered a second discrete conversation. Depending on the agency's undercover guidelines and the sensitivity of the operation, the agent may need to obtain approvals under the agency guidelines before engaging in further undercover communications on this matter.

PRINCIPLE 7

ONLINE UNDERCOVER FACILITIES

Just as law enforcement agencies may establish physical-world undercover entities, they also may establish online undercover facilities, such as bulletin board systems, Internet service providers, and World Wide Web sites, which covertly offer information or services to the public. Online undercover facilities, however, can raise novel and complex legal issues, especially if law enforcement agents seek to use the system administrator's powers for criminal investigative purposes. Further, these facilities may raise unique and sensitive policy issues involving privacy, international sovereignty, and unintended harm to unknown third parties.

Because of these concerns, a proposed online undercover facility, like any undercover entity, may be established only if the operation is authorized pursuant to the agency's guidelines and procedures for evaluating undercover operations. In addition, unless the proposed online undercover facility would merely provide information to members of the public or accounts to law enforcement agents, the agency or federal prosecutor involved in the investigation must consult in advance with the "Computer and Telecommunications Coordinator" (CTC) in the United States Attorney's office in the district in which the operation will be based, or with the Computer Crime and Intellectual Property Section (CCIPS) of the Justice Department's Criminal Division. An attorney from the Section can be reached at (202) 514-1026 or through the Justice Command Center at (202) 514-5000.

Agencies that already consult with the Justice Department as part of their internal review process for undercover operations may comply with this requirement by providing an extra copy of the undercover proposal to the CTC or to CCIPS, as appropriate.

COMMENTARY

A. The Definition of Online Undercover Facility

As discussed in **Principle 6, Undercover Communications**, law enforcement agencies establish undercover operations in order to prevent serious crimes and to procure otherwise unobtainable evidence. In some instances, it is appropriate for law enforcement agencies to

establish covert businesses or other entities to gather evidence of criminal activity. Internal agency guidelines generally establish a review process by which such proposals are carefully evaluated and the conditions for their authorization are prescribed.

Law enforcement agents may propose creating undercover entities not only in the physical world, but also online. The same agency guidelines, procedures, and policies used to evaluate and authorize other kinds of undercover entities must be followed for proposals to establish online undercover facilities. In addition, however, online undercover facilities can raise special concerns, as discussed below. Because of those concerns, proposals for the establishment of certain kinds of online undercover facilities must also be evaluated by Federal prosecutors with the most experience in this area: the "Computer and Telecommunications Coordinator" (CTC) in the United States Attorney's office in the district in which the operation will be based, or the Computer Crime and Intellectual Property Section (CCIPS) of the Justice Department's Criminal Division.[25]

For purposes of this Principle, an "online undercover facility" includes a service provider, web site, or similar facility that is covertly run or controlled (directly or indirectly) by law enforcement and is intended to provide services to individuals who do not know that they are dealing with law enforcement. Thus, online facilities that provide accounts or information only to individuals who know that the system is operated by law enforcement are not online undercover facilities. An example of such an excluded facility is a system run by law enforcement agencies solely to provide accounts (for Web access or e-mail registered in an undercover name) to agents. For the same reason, an Internet account that an agent establishes with a public Internet Service Provider under his or her undercover identity also does not fall within the definition.

---

[25] Nothing in this Principle requires information to be disclosed in a manner prohibited by law. For example, Section 6103 of the Internal Revenue Code prohibits the disclosure of tax return information to prosecutors prior to a "referral" of a matter to the Department of Justice. The submission of a proposal that contains tax return information to the CTC or to CCIPS under the consultation requirement must be made in accordance with the referral and disclosure rules provided by the statute and agency guidelines.

Importantly, there are some online undercover facilities that do not require consultation with the CTC or with CCIPS. Specifically, consultation is not required if the online undercover facility merely provides information or a means to contact agents. This exception is discussed below in Section C, The Scope of the Consultation Requirement.

Finally, online facilities that are not run by federal law enforcement agencies for criminal investigative purposes _ such as state and local law enforcement online facilities, and federal administrative, intelligence or counterintelligence operations _ are not within the scope of this Principle. (See Overview, at page 2.) However, federal agents participating in task forces or joint operations with state or local law enforcement officers who are operating online undercover facilities should consult with CCIPS or their local CTC in order to identify any special issues the joint operation may raise.

B. Special Concerns Arising from the Operation of an Online Undercover Facility

Law enforcement agencies must consider several novel and especially sensitive issues when determining whether to approve the establishment of a proposed online undercover facility.

First, online undercover facilities that offer the public access to information or computer programs that may be used for illegal or harmful purposes may have greater capacity than similar physical-world undercover entities to cause unintended harm to unknown third parties. Because digital information can be easily copied and communicated, it is difficult to control distribution in an online operation and so limit the harm that may arise from the operation.

To illustrate this difference, compare the features of a physical world facility with those of an online undercover facility. An example of a physical world undercover facility might be a storefront to sell "clone phones" to individuals involved in cellular telephone fraud. Agents operating such a facility can prevent or minimize the potential for harm caused by their activities by, for example, arresting targets before they can use the phones or requesting the cellular carrier to block or limit access by these particular phones to the cellular network. Even absent such measures, the harm that can arise is constrained by the physical nature of the object involved in the transaction: a single "clone phone" can only be used by one individual at a time and cannot be duplicated and redistributed to multiple users.

An analogous online undercover facility might be a web site that offers "hacker tools" (programs designed to penetrate computer systems) which is covertly run by law enforcement to

discover criminals who are using such tools to break into computer systems. The online facility is likely to be automated, making it difficult for the agents to limit who obtains the tools or the damage that the tools end up causing to innocent third parties. Further, unlike the clone phone, the hacker tools can be endlessly replicated and distributed to others in a manner that law enforcement agents cannot easily control.

Second, online undercover facilities have a greater potential than comparable physical-world facilities to invade the privacy of innocent visitors or participants. Again, selling clone phones from a storefront would have little effect on the privacy interests of the few people who might try to transact legitimate business with the undercover agents. By contrast, citizens who visit a web page may feel that their privacy has been violated if they eventually discover that the government was secretly running the web page and keeping track of the visitors to the site.

Third, the operation of online undercover facilities may raise difficult legal issues when law enforcement agents seek to use the legal authority of system administrators for criminal investigative purposes. That is because law enforcement agents and system administrators have different statutory rights and obligations in obtaining electronic information. Generally, the Electronic Communications Privacy Act (ECPA) places strict limits on when and how law enforcement agents can obtain various kinds of information from electronic service providers (such as Internet service providers). In general and subject to certain exceptions, this statute requires law enforcement to obtain a wiretap order to monitor real time communications (18 U.S.C. § 2518), a search warrant to access the contents of electronic communications in electronic storage (18 U.S.C. § 2703(a)), and a court order or subpoena to obtain transactional data (18 U.S.C. § 2703(c)(1)(B)).

The system administrator of an electronic communication system, by contrast, may, without a court order, conduct real-time system monitoring to render service or protect the rights and property of the provider. 18 U.S.C. § 2511(2)(a)(i). ECPA also explicitly permits system administrators to examine stored electronic communications, 18 U.S.C. § 2701(c)(1), and does not restrict their access to transactional data.

Law enforcement agents may not circumvent the statutory restrictions on government access to information simply by covertly becoming a service provider. Thus, while law enforcement agencies may use the system provider's authority to manage or protect the system, they may not use the system administrator's legal powers to gather evidence normally obtainable only through procedures required by ECPA. To avoid legal complications, agencies should

consider taking steps to separate the responsibility for administering the online facility, to which one legal framework applies, from its criminal investigative function, to which a different legal framework applies.

Fourth, the creation of any kind of online undercover facility, even one (like a non-interactive web page) that is merely the online equivalent of a classified advertisement, may have unintended but unavoidable national and international repercussions. Most undercover entities in the physical world have only a local effect, attracting responses only from the district or region in which the operation is being conducted. The worldwide communications provided by the Internet, by contrast, make it difficult for agents to limit online access to local or even domestic targets, and they are likely to log inquiries coming from anywhere in the world. While investigating targets located in other jurisdictions within the United States may raise some questions of enforcement priorities or tactics, investigating people located in other countries raises far more sensitive international concerns, particularly if the operation results in harm to third-party victims abroad. See **Principle 11, International Issues**.

Finally, agencies must be sensitive to the profound public policy implications that can be raised by online undercover facilities. Imprudent or undisciplined use of such facilities by any agency will surely lead to public distrust of law enforcement's online work in general.

C. The Scope of the Consultation Requirement

In light of these novel and sensitive legal and practical concerns, agencies contemplating any kind of online undercover facility, and any federal prosecutor assigned to the investigation, are encouraged to consult early in the process with the Computer Crime and Intellectual Property Section (CCIPS) of the Justice Department's Criminal Division (202-514-1026), or with a "Computer and Telecommunications Coordinator" (CTC) in the United States Attorney's office in the district in which the operation is based. The CTCs are Assistant United States Attorneys who work closely with CCIPS and have been given special training in, and are responsible for, computer-related legal issues within their districts. Each United States Attorney's office has at least one CTC. Agents may obtain the name of a District's CTC from the United States Attorney's office or from CCIPS.

Consulting with CCIPS or with the CTC will provide the investigative agency considering the proposal with important information on rapidly developing issues unique to this area, including statutory restrictions and recent case law. The consultation also will ensure that the

agency is fully informed of issues that have arisen in similar operations, and of other legal and practical problems that might arise in the proposed operation.

For certain types of online undercover facilities, consultation with CCIPS or the CTC is required. Agencies or an assigned federal prosecutor must consult with CCIPS or the local CTC unless the proposed online undercover facility only provides information or a means to contact agents. Specifically, consultation is not required before an agency sets up a web page that operates like a physical-world billboard, simply advertising the existence of a business or an apparently illegal scheme and providing a contact point for further inquiry, such as a telephone number or an e-mail address. Consultation is not required to establish such facilities so long as they do not, for investigative purposes, collect or process information about anyone who connects to the system without knowing it is run by law enforcement.

D. The Operation of the Consultation Requirement

When a proposed online undercover facility requires consultation, this requirement may be met by the agency or an assigned federal prosecutor consulting either with the CTC in the district in which the operation will be based, with CCIPS, or with both.[26] Agencies and prosecutors are encouraged to consult with the CTC or CCIPS early in the approval process, so that potential issues can be fully identified and considered. In this consultation, CCIPS or the CTC can alert the agency or prosecutor to any international issues and discuss those issues with the Office of International Affairs. In any event, unless an emergency situation prevents it, the CTC or CCIPS should be given sufficient time to conduct a meaningful review and notify the agency of any substantial issues of law or policy that the CTC or CCIPS identifies.[27]

To minimize potential misunderstandings about how the proposed online undercover facility would operate, the proposal provided to the CTC or CCIPS must be reduced to writing.

---

[26] The guidelines that govern some agencies permit initial approval of certain kinds of undercover operations on a local level, but require more costly or sensitive operations to be referred to headquarters for approval. Agencies and the prosecutor with whom they are coordinating may, at their discretion, wish to have the CTC consult on locally reviewed operations and CCIPS review operations reviewed by headquarters.

[27] CTCs are reminded to follow their own office policies and notify the appropriate supervisor in the U.S. Attorney's Office when they are consulted under this Principle.

At the agency's discretion, the proposal may be the same internal document used by the agency's reviewing authority.[28] Agencies that already consult with the Justice Department as part of their internal review process for undercover operations may comply with this requirement by providing an extra copy of the undercover proposal to the CTC or to CCIPS, as appropriate.

> ***EXAMPLE 1***: As part of a project to identify and prosecute computer criminals, a law enforcement agency considers a proposal to operate a World Wide Web site with information about and computer programs for hacking, links to other hacker sites, and a facility to allow people who access the site to discuss hacking techniques. The proposal would allow the law enforcement agents running the site to track all visitors, and monitor all communications among the users. Because this proposal would establish an online undercover facility that would do more than just provide information or a means to contact agents, the consultation requirement applies to this proposal.
>
> In considering the proposal, the agency should recognize that operating such a site raises all the issues discussed in the Commentary. Specifically, the agents may have little or no ability to prevent harm to third parties caused by distribution of information from the site or the tools from the linked sites; the tracking may result in the investigation of innocent visitors to the site, such as computer security professionals or reporters; ECPA governs the extent to which investigators are permitted to monitor communications among users of the facility; and harm could extend to overseas victims, raising potential international concerns.

---

[28] While this consultation requirement only applies to online undercover facilities that are established after these Principles are issued, agencies are encouraged to inform CCIPS or the local CTC of any ongoing online undercover facility it is operating, if the operation had not previously been discussed with CCIPS or the local CTC.

***EXAMPLE 2*:** As part of an undercover operation, a law enforcement agency has set up a business entity purporting to sell protected animals to zoos and collectors in order to identify and investigate individuals who are illegally trafficking in such animals. The agents intend to promote the business through a World Wide Web site that advertises the business and provides a mechanism that allows visitors to the site to contact the agents by e-mail.

Because the site is designed merely to advertise electronically and provide a means to communicate with the undercover agents, consultation with CCIPS or the local CTC is encouraged but not required. Consultation is not required if the system operator of the Web site intends to log visits to the site for system administrative purposes only.

Regardless of whether consultation is required, the agency should fully evaluate the risks identified in the Commentary when reviewing the proposal. For example, because their site will be available internationally, agents may become involved in negotiations with vendors to purchase animals that cannot legally be imported into the United States but may be lawfully captured and sold in the country where the vendor is located.

***EXAMPLE 3*:** A law enforcement agency proposes to set up and operate an Internet host to provide e-mail accounts and World Wide Web access for its undercover agents. No other customers will be allowed to open an account or access information. The system administrator will not collect any investigative information, but will simply enable the communications to and from the undercover agents. Because the facility is intended to provide accounts only to individuals who know that the system is operated by law enforcement, its operation does not require consultation.

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.

COMMENTARY

One of law enforcement's longstanding weapons against crime has been enlisting cooperating witnesses to communicate with, and sometimes to record face-to-face or telephonic conversations with, the subjects of investigations. The Supreme Court has upheld this technique, recognizing that a criminal assumes the risk that his trust in his confederate may be misplaced. See Hoffa v. United States, 385 U.S. 293 (1966). In addition, because the cooperating witness, as a party to the communication, may properly divulge the contents of the conversation to law enforcement, he or she may also record the conversation as a more accurate rendition of the dialogue. The Wiretap Statute expressly recognizes that recording a wire, oral, or electronic communication with the consent of a party does not violate federal law. 18 U.S.C. § 2511(2)(c), (d).

Consensual communications that occur online are not conceptually different from other types of consensual communications, and should be treated the same under agency regulations or procedures. Just as an individual orally discussing a past or future criminal activity assumes the risk that the other party is cooperating with law enforcement and recording the conversation, the individual engaged in an electronic dialogue with a party assumes the same risks.[29]

[29] Indeed, online conversations introduce an added element of risk to the parties. In the physical world, a person communicating with someone he or she knows can recognize the other person's face or voice. By contrast, a person communicating online generally cannot see or hear

the other parties to the communication, but (in most cases) can identify others only through their usernames, which is unreliable because they can be forged. Thus, absent a trusted authentication measure (such as digital signatures), the online user can never know for certain the true identity of the other person sitting at the keyboard.

Although these considerations are similar regardless of whether it is the cooperating witness or the agent who is actually typing at the keyboard, the difference may be important for purposes of agency guidelines. An agent using a cooperating witness's identity is representing herself as someone else, and thus is acting under an assumed name or fictitious identity. As discussed in **Principle 6, Undercover Communications**, such an agent is bound by the undercover guidelines of her agency which may, depending on the nature, extent, and sensitivity of the contacts, impose certain restrictions on her activities and/or require her to obtain whatever approvals are required by her agency. Special approvals may be required if the agent is communicating with foreign contacts or engaging in foreign undercover activities. See **Principle 11, International Issues**.

If the cooperating witness permits a law enforcement agent to communicate through the witness's online identity, it is crucial to come to a clear understanding of the precise scope of the witness's consent. For example, the witness may consent to the agent's using his or her identity only to send or receive e-mail, upload postings, or download certain files. Or he may allow the agent to communicate with operators of online services that illegally distribute copyrighted works. If an agent, without obtaining further consent, were to then use that witness's online identity to engage in other activity not consented to — such as downloading child pornography — the agent arguably would be appropriating the witness's identity beyond the scope of the witness's consent. This would raise the difficult issues addressed in **Principle 9, Appropriating Online Identity**. To avoid such issues, it is recommended that the agent and cooperating witness agree in writing on the scope of the witness's consent, and make certain the agent abides scrupulously by that agreement.[30]

EXAMPLE: A recipient of child pornography decides to cooperate with the government. If the cooperator consents and approval for consensual monitoring is obtained, the

[30] In order to avoid confusion over who is responsible for particular communications, the agreement should also specify whether and under what circumstances the witness may use his or her own online identity during the same period it is being used by federal law enforcement agents.

cooperating witness may communicate electronically with others and log those conversations in order to obtain information pertinent to a criminal investigation. If the cooperating witness agrees to allow the law enforcement agent to assume his online identity for the purpose of communicating about child pornography, the agent and the witness should agree in writing on the scope of the consent. Communications by the agent through the witness's online identity should be considered undercover activity, subject to authorization by the agency.

PRINCIPLE 9

APPROPRIATING ONLINE IDENTITY

"Appropriating online identity" occurs when a law enforcement agent electronically communicates with others by deliberately assuming the known online identity (such as the username) 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. To appropriate online identity, a law enforcement agent or a federal prosecutor involved in the investigation must obtain the concurrence of the United States Attorney's Office's "Computer and Telecommunications Coordinator" (CTC) or the Computer Crime and Intellectual Property Section. An attorney from the Section can be reached at (202) 514-1026 or through the Justice Command Center at (202) 514-5000. In rare instances, it will be necessary for law enforcement agents to appropriate online identity immediately in order to take advantage of a perishable opportunity to investigate serious criminal activity. In those circumstances, they may appropriate identity and notify the Computer Crime and Intellectual Property Section within 48 hours thereafter.

COMMENTARY

A. Appropriating Online Identity as a Law Enforcement Technique

When acting undercover, law enforcement agents usually communicate with third parties by assuming a fictional identity,[31] or occasionally by assuming the identity of a cooperating witness after obtaining that witness's consent.[32] "Appropriating online identity" occurs when a law enforcement agent electronically communicates with a third party by deliberately assuming the known online identity of a real person without obtaining that person's consent.

---

[31] See **Principle 6, Undercover Communications**.

[32] See **Principle 8, Communicating Through the Online Identity of a Cooperating Witness, with Consent**.

Law enforcement agents rarely appropriate identity in face-to-face or telephone communications, because it is very difficult to replicate the face or voice of another person in a convincing manner. It is much easier, however, to impersonate someone else when law enforcement agents use online resources to communicate: parties communicating electronically identify each other primarily by usernames and other non-physical methods, thus making the deception easier. Moreover, there are a number of computer techniques that can assist an electronic impersonation, permitting agents to send information that appears to come from a particular user.

Appropriating online identity is a highly intrusive law enforcement technique that can invade the privacy and damage the reputation of the person whose identity has been appropriated, invade the privacy of a third party unaware that he or she is communicating with a law enforcement agent, and raise significant legal problems. The technique should be confined only to investigations of serious criminal cases, and should be used in those investigations as narrowly as possible. The Justice Department, when evaluating whether to concur in a proposal to appropriate identity, will consider the interests affected by the use of the technique and its potential value in the criminal investigation in question, including the availability of less intrusive investigative methods.

There are a number of reasons that appropriating identity deserves special scrutiny. First, a person's reputation can obviously be damaged whenever his or her identity is appropriated. There have been increasing press reports about individuals whose online identity have been appropriated by someone else to communicate false information or offensive messages in the victims' names. As a result, these people have suffered damage to their reputations, their privacy, and sometimes even their safety. The damage caused may be both long-lasting and widespread, because any communication appearing to originate from a particular person can be preserved and forwarded to many others over time.

Second, when a law enforcement agent appropriates online identity in order to communicate with a third party, the privacy interests of that third party may be affected. The usual justification for consensual monitoring is that a person assumes the risk that his or her "trust" in the discretion of a criminal confederate may be misplaced. This justification fits uncomfortably where a law enforcement agent has inserted himself into that trust relationship without the consent of either party.

Third, appropriating online identity may raise statutory and constitutional issues that are simply not present when agents appropriate identity in the physical world. An agent's use of a telephone to pretend to be someone else generally does not require any special technical efforts.

In order to communicate electronically in the name of another, however, the agent must usually either forge that person's online address, break into his online account, or come into possession of and use his online password.

Forging the online address of another or breaking into his account may require agents to use tools, programs, and commands to breach the security or access restrictions of a computer system in a manner that would be illegal if used by others, potentially raising difficult statutory and Fourth Amendment issues.[33] Even an agent who logs on by using another person's password that is lawfully in the agent's possession risks receiving statutorily protected communications (such as e-mail or instant messages) for which the agent is not the addressee or intended recipient, raising questions under Electronic Communications Privacy Act (ECPA). Logging on may also cause e-mail to be downloaded from the Internet service provider to the machine used by the investigator, arguably a search of the service provider in violation of ECPA or the Fourth Amendment.

Use of a defendant's computer or account could also raise serious evidentiary issues. For example, a defendant may allege that the agent has tampered with or altered evidence by using the defendant's computer or account.

Finally, the use of an appropriated identity in any situation involving international concerns should be reviewed consistent with previous guidance and reference to **Principle 11, International Issues**.

[33] Additionally, such an attack, if detected by the administrator of the system, might result in a referral to federal, state, or local law enforcement authorities, who would then begin an investigation of the perceived "intrusion."

B. Department of Justice Approval for Appropriating Online Identity

Because of the important concerns raised above, and to ensure that this technique is used properly, an agent or prosecutor involved in the investigation must, whenever possible, seek the concurrence of the United States Attorney's Office's Computer and Telecommunications Coordinator (CTC) in the District where the investigation is taking place or the Justice Department's Computer Crime and Intellectual Property Section (CCIPS) before appropriating online identity.[34] An attorney from the Section can be reached at (202) 514-1026 (during business hours) or through the Justice Command Center at (202) 514-5000 (24 hours a day).

There may be rare emergencies or exigent circumstances in which law enforcement agents need to appropriate online identity in order to take advantage of a perishable opportunity to investigate or prevent serious criminal activity but do not have time to contact the CTC or CCIPS in advance. In those circumstances, they may appropriate identity and notify the CTC or CCIPS as soon as possible after assuming the identity of another without consent, and in no event more than 48 hours thereafter.

EXAMPLE 1: Law enforcement agents learn the username of a drug kingpin who communicates with members of his organization through e-mail. The agents develop a long-term plan to forge the drug kingpin's user name and send e-mail messages to these members, convening a meeting. The plan to appropriate identity must be submitted for concurrence to the Department of Justice, through the Computer Crime and Intellectual Property Section or the CTC in the District where the investigation is taking place.

EXAMPLE 2: Agents executing a search warrant on a drug dealer's residence learn (from, for instance, an interview of an accomplice present at the residence or a lawful search of a computer on the premises) that the drug dealer's supplier is expecting the suspect to send him an e-mail confirming a proposed sale within the next few hours. The agents want to send an e-mail message purportedly from the dealer instructing the supplier to deliver the drugs to the dealer's residence. Using the dealer's computer, with

[34] CTCs are reminded to follow their own office policies and notify the appropriate supervisor in the U.S. Attorney's Office when they are consulted under this Principle.

an embedded password and a dial-up script to the online account, the agents have the technical ability to send the message.

Accessing the drug dealer's online account without his permission may raise a number of issues, including issues under the Fourth Amendment and under various provisions of the Electronic Communications Privacy Act. The agents should contact the Department of Justice, through the Computer Crime and Intellectual Property Section or the CTC in the District where the investigation is taking place, to obtain concurrence to appropriate the dealer's identity. A Section attorney or other Department official can be reached 24 hours a day. During working hours agents may call 202-514-1026, and at all other times may call the Justice Command Center (202-514-5000).

EXAMPLE 3: Law enforcement agents learn that a drug dealer is arranging for the murder of a former co-conspirator who he suspects is cooperating with the government. They also learn that the drug dealer is expected to confirm the order with an imminent e-mail message. The agents wish to send an e-mail message purportedly from the drug dealer delaying the execution so that they have time to warn the intended victim, but do not have time to contact the Computer Crime and Intellectual Property Section or the CTC. The agents may appropriate identity and then notify the Computer Crime and Intellectual Property Section or the CTC in the District in which the investigation is taking place as soon as possible, and at least within 48 hours after they appropriate identity.

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 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.

COMMENTARY

Agents' off-duty use of online resources raises important — and sometimes competing — concerns. On one hand, agents should be able to take advantage of the activities and information available on the Internet and other networks. Both common sense and the First Amendment compel a rule that allows agents to engage in some personal pursuits online. On the other hand, government must control agents' investigative activities. Absent such control, after-hours activity runs the risk of circumventing the restrictions imposed by these Principles and by applicable agency guidelines.

This Principle strikes a balance between these differing interests. Agents are allowed to engage in personal online pursuits on the agent's personal time without being subject to the agency's rules and policies governing investigative conduct, even if they are pursuing online activities that enhance their skills or knowledge relating to their duties. When the activity is aimed at the development or pursuit of investigative leads, however, they should be considered on duty and subject to the agency's rules and policies governing investigative conduct, regardless of whether the investigative activity is occurring during working hours or from the workplace.

Agents should be encouraged to use their personal time to enhance their skills. In many cases, an agent's need or desire to stay current on duty-related subjects — whether legal or technical — will motivate online activity during personal hours as well as work hours. This may be especially true for agents whose official duties involve the investigation of computer network crimes, given the constantly changing character of both the medium and the underlying technology. A contrary rule — one that forbids using personal time for online activity related to duty-related subjects — would disserve both the agents' First Amendment rights and the development of their online skills.

The critical distinction here is between enhancing overall knowledge and developing or pursuing specific investigative leads. Existing agency regulations impose stringent limits on the use of personal time to conduct active investigations: for example, an agent may generally not stake out a suspect's home on his own initiative during off-duty hours. However, agencies do not restrict an agent's use of off-duty time to read about stake-out strategies or surveillance methods in general.

In the online world, of course, it may take far less effort — and involve fewer risks — for an off-duty agent to investigate a case. But the ease of doing so must not override the important reasons for ensuring that the agent follow agency guidelines while investigating, such as an agency's need to oversee the activities of its agents. On the contrary, when an agent's use of the Internet or other online facilities rises to the level of investigative activity, the agent should be considered on duty and subject to the same rules and policies that govern investigative conduct during normal working hours.

Even when agents' personal online pursuits are clearly not tied to duty-related subjects, certain restrictions apply in the same manner as to other off-duty conduct. To the extent agents engage in personal online pursuits using equipment or an online address issued by the agency, they should be careful to comply with agency policy on their use. Even when using personal equipment or a personal online account, agents must comply with Office of Government Ethics Standards of Conduct for Government Employees relating to outside activities, any supplemental agency regulation, as well as the Office of Personnel Management's prohibition on any employee engaging in "criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, or other conduct prejudicial to the Government." Note that when an agent engaged in personal online pursuits observes or finds out about criminal activity, the agent should report it as required.

> ***EXAMPLE 1:*** During personal time, an agent using a personal account to participate in an online discussion group devoted to hunting. So long as the agent adheres to general agency guidelines regarding conduct during personal hours, the agent may participate in this group in the same manner as any other citizen. If, however, the agent observes a discussion that indicates unlawful activity — for example, the planned sale of unlicensed fully automatic weapons — then the agent has the same duty as under other off-duty circumstances to report that information.
>
> ***EXAMPLE 2:*** An agent's official duties include investigating computer crimes. The agent has an avid interest in computer security issues, and subscribes to an electronic mailing list that reports and discusses newly discovered "bugs" in software. So long as the agent's reason for participating in the mailing list is to keep abreast of technical developments in the area, then the agent's activity is not subject to agency restrictions on

investigative conduct. If the agent subscribes in order to observe hackers planning criminal activities, however, then the agent is covered by the agency rules and regulations governing investigations to the same extent as during regular duty hours.

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.

COMMENTARY

A. International Investigations in an Online World

To an ever-increasing extent, criminal activities and organizations are becoming international in scope. As a result, U.S. law enforcement agencies often must obtain information from, and investigate citizens of, other countries. Naturally, this type of law enforcement activity raises extremely sensitive issues of national sovereignty and foreign policy — just as it does when foreign law enforcement agencies investigate in the United States. Therefore, law enforcement agencies, in conjunction with the Justice Department's Office of International Affairs, have carefully developed policies and procedures for their agents to follow in matters that cross international boundaries.

The emergence of international computer networks is greatly exacerbating the already considerable difficulties agents face in conducting international investigations for two reasons. The first is that the expansion of online resources and facilities makes it easier to commit crime on an international scale, increasing the quantity of international crime and straining the mechanisms used to address it. The second is that the same rapid and easy connectivity and absence of physical boundaries that make the online world easy to use often make it extremely difficult for law enforcement agents even to recognize that they have crossed a border.

The U.S. government is working with other countries to increase cooperation among law enforcement agencies in the information age. Given the complexities and sensitivities of the issues, and the differing views among even our close allies about core concepts, easy solutions are not at hand. In the meanwhile, the quick march of technology makes the task of detecting and solving international computer-related crime ever more complicated and urgent.

B. Obligations of Law Enforcement Agents in Online Investigations

Except when accessing information from facilities configured for public access, as discussed in **Principle 1**, **Obtaining Information from Unrestricted Sources,** law enforcement agents conducting online investigations should use reasonable efforts to ascertain whether a pertinent computer system, data, witness, or subject is located in a foreign jurisdiction. Whenever agents find that one of these is located outside the United States, they should follow the procedures set out by their agencies for foreign contacts. These procedures may include consulting — either directly or through the relevant prosecutor — with the Justice Department's Office of International Affairs (OIA), who are experts in investigations that raise transborder issues. The telephone number for OIA is 202-514-0000. In light of the complexities and sensitivities of these investigations and processes, and the difficulties inherent in ascertaining physical location in an online environment, law enforcement agents should not hesitate to seek guidance if they suspect a transborder issue may arise.

Although the Principle applies equally whether agents are focusing on foreign systems and data, witnesses and informants, or subjects of investigations, slightly different issues are raised by each situation. Additionally, it is useful to note separately issues raised by undercover operations, lures, and e-mails.

Systems and Data. Most major U.S. law enforcement agencies have established procedures to obtain physical evidence located outside the U.S., generally by working with law enforcement officials in the country where the evidence is located. Unless there are international agreements to the contrary, those same procedures should be employed when agents seek information stored electronically in computers located in another country.

Agents usually know where international boundaries are physically located, but those boundaries are not so obvious in a networked environment. For example, executing a search warrant for certain computer files from a multi-national company in the U.S. may result in downloading information from a server located outside the U.S.

Analogizing from the principles that govern the seizure of physical evidence, downloading information from a foreign computer during the search of a domestic computer is considered by many to constitute a transborder search, on the theory that any information accessed from a particular computer should be considered as having been seized from the jurisdiction where that computer is physically located. While application of this physical-world analogy to the realities of network storage is the subject of ongoing controversy and negotiation, for the present agents should continue to regard downloading from a server located in another country as a search of a foreign location.

Clearly, using established procedures to obtain electronic evidence located outside U.S. borders will be time-consuming and cumbersome, and may put the collection of the evidence at risk. The U.S. and other nations are working hard to accelerate and streamline the process for obtaining electronic evidence. While this effort is underway and this issue is being debated in a variety of international contexts, U.S. law enforcement agents must respect the territorial sovereignty of other nations, just as we expect foreign law enforcement agents to respect ours.

Accordingly, agents should always make reasonable efforts to find out where the relevant electronic records are stored. If they learn before or during the search that the information may be stored in servers outside the United States, they must proceed as they would to obtain physical evidence located outside the U.S. If agents later discover they have inadvertently downloaded information from servers located abroad, they should seek immediate guidance from those authorities within their agencies who handle obtaining evidence from foreign nations.[35]

Agents should also be careful about obtaining records or documents stored electronically when working with a cooperating witness. At one extreme, a cooperating witness located in the U.S. may generally provide U.S. law enforcement authorities with access to her own records that happen to be stored outside the U.S. In that circumstance, the witness is merely exercising her personal right to access her own documents. Other examples provide closer cases. For instance, a cooperating witness may be authorized to access electronic copies of company documents and records strictly for work-related purposes. Fourth Amendment issues may be raised if the witness instead accesses those records for law enforcement purposes. If the records are stored outside the U.S., the witness's providing them to U.S. law enforcement may also implicate sensitive international issues. Agents should consult their agencies and the federal prosecutor assigned to the case before taking such records or asking a cooperating witness to access them.

Witnesses and Informants. Geographic boundaries play little part in global networks. An agent investigating an intrusion into a computer in Iowa, for example, is as likely to find

[35] Sometimes, the information on a server located in another country may have been previously copied to servers in the U.S. by the target or some third party. Obtaining information from the U.S. server would alleviate the international concerns identified in this Principle.

witnesses and informants from Denmark as from Des Moines. Moreover, because it is easy to alter or conceal online identity and location, the agent may not know where the witness or informant is.

Despite these difficulties, agents should try to find out where witnesses and informants are before they communicate with them.[36] Witnesses who appear to be abroad must be handled according to agency procedures for dealing with foreign witnesses. Because these rules and the sensitivities they raise vary from country to country, agents should exercise great care.[37] There may be a variety of reasonable ways to determine the location of witnesses and informants, including asking the witness or informant where he or she lives, and checking publicly available information, such as the country of the witness's Internet service provider. Of course, as technology continues to evolve, what constitutes a reasonable effort to establish location is likely to change.

---

[36] It is important to emphasize that the obligation to take reasonable steps to determine if a witness or subject is located in a foreign jurisdiction applies only when law enforcement agents plan to contact that witness or investigate that subject. Law enforcement agents have no obligation, for example, to track down the location of someone who responds to a solicitation to participate in a chain letter scheme that is posted by a law enforcement agency in an undercover operation if the agent is not planning to investigate or contact that person.

[37] Obviously, the sensitivities are lessened if U.S. law enforcement consults with and receives permission from our foreign counterparts before contacting a foreign witness. U.S. law enforcement agents have relationships, arrangements, and agreements with foreign law enforcement agents in a number of countries; these Principles are not meant to alter those relationships, arrangements, or agreements.

It should be stressed that this Principle does not bar contacts with witnesses or informants from outside the U.S. Rather, it simply directs agents to follow the same procedures online as they would in person or over the telephone, mindful of the sensitivities of, and potential penalties that could be imposed by, a foreign sovereign.

Subjects. Agents also should try to establish, at the earliest possible juncture, whether the subject of their online investigation is located abroad. There are important practical reasons for this. Obviously, in order to solve a crime and bring the perpetrator to justice, agents must determine his true identity and location. When the perpetrator is located in another country, agents must work with law enforcement officials in that foreign jurisdiction. Those officials may have useful information about the subject, and their assistance will be required to collect evidence in that country, to prosecute the subject, or to extradite him.

In cases involving foreign subjects in online investigations, governments are often especially sensitive about their sovereignty and the rights of their citizens. We must do our utmost to avoid investigative actions that may create problems with foreign counterparts for years to come. If in doubt, agencies or the assigned prosecutor should consult with OIA.

Undercover Activities and Operations. As noted in the **Principle 6, Undercover Communications** and **Principle 7, Online Undercover Facilities**, online undercover operations run a much greater risk than other kinds of undercover operations of inadvertently involving foreign subjects or witnesses. Foreign subjects and witnesses are likely to complicate an undercover operation, and foreign nations may be even more concerned about contacts with their citizens when U.S. law enforcement agents do not identify themselves as such. To the extent possible, the design of the undercover operation should consider the risk and the effect of responses from foreign locations. Again, when in doubt, consult with OIA and the Justice Department's Computer Crime and Intellectual Property Section (202-514-1026).

Lures. When communicating online or otherwise with a subject or target, either directly, in an undercover capacity, through a cooperating witness or informant, or via an assumed identity, any communication to entice a person to travel from one country to another for purposes of apprehension must be approved through the relevant agency and by the Assistant Attorney General for the Criminal Division.

Use of E-mail and other types of electronic communications. Because international electronic communications are so effortless, it is easy to forget that they are international. As set out in **Principle 5, Online Communications _** Generally, such communications are covered by the agency's regulations on other sorts of international communications, such as telephone

contacts. Agencies may require approval or consultation before contacts are made with witnesses, informants, or subjects located abroad.

> ***EXAMPLE 1:*** Law enforcement agents obtain a warrant to search the Buffalo, New York, branch office of a Canadian-based company for fraud-related documents that may be stored on computers. The agents should take reasonable steps, such as interviewing cooperating witnesses, to determine if the documents to be seized may be stored exclusively on a server in Canada. If they know or have reason to believe that evidence is stored only outside the U.S., the agents must follow agency procedures for obtaining evidence located in a foreign jurisdiction.
>
> ***EXAMPLE 2:*** Law enforcement agents investigating an attack on a U.S. computer system are authorized by their agency to monitor an IRC channel that the suspects are known to frequent. One of the participants suggests that he or she has knowledge about the attack. The agents should use reasonable means to determine if the witness may be outside the U.S. If so, the agents should follow the agency's policies and procedures for dealing with foreign subjects or witnesses before contacting the potential witness/subject on either an identified or undercover basis.

APPENDIX A: THE ONLINE WORLD AND LAW ENFORCEMENT

To understand and apply these Principles, law enforcement agents need a basic understanding of the kinds of activity they may encounter online. This Appendix introduces the Internet and other online resources. In addition, it provides a summary of the most common types of illegal online conduct.

A. Internet Resources and Services

"The Internet" is a phrase with multiple meanings. It refers to a physical infrastructure (computers, data transmission cables, and related network hardware); to the data available on the physical network (including not only text but also graphics, audio, and video files as well as applications programs) and the means of locating and retrieving that data; or even to the people who use the physical network. This section offers a brief overview of the different aspects of the Internet (and other online facilities) relevant to law enforcement investigations, along with an explanation of the relationships among these component parts.

1. The Physical Layer

At its most basic level, the Internet is a worldwide network of hundreds of thousands of computers. It includes computers owned by universities, nonprofit organizations, governments, corporations, and individuals. The types of computers (ranging from PCs to large mainframes) and communications links (from standard phone lines to satellite hookups) vary widely, as do the types of software used. These computers share only one common characteristic: they communicate with each other using a single standard protocol.

There is no central authority that controls the Internet or access to it. Instead, the network is administered in a largely decentralized fashion, with each site collaborating primarily with its closest neighbors. This arrangement reflects a deliberate decision in designing the Internet's domestic predecessor, the Defense Department's Advanced Research Projects Agency network (ARPANET), to create a decentralized network able to remain in operation even when an individual site is disabled (by hostile foreign action, for example).

Each Internet site has a unique two-part name that normally reflects the site owner's identity. For example, the International Business Machines site is IBM.COM, where the .COM suffix indicates a commercial organization. Other common suffixes are .EDU (for universities), .GOV (U.S. government), .MIL (U.S. military), .NET (for network access providers), and .ORG (nonprofits and other miscellaneous entities). In addition, many sites outside the U.S. have name suffixes indicating the location of the machine and/or its owner-organization, such as .UK (United

Kingdom) and .DE (Germany). However, many foreign sites do not have geographical identifiers in their names; thus, one cannot assume that a .COM site belongs to a company in the U.S. Further, even where a site does have a geography-based suffix (such as .US), there is no guarantee that the computers associated with that site are in fact located in the specified country.

Within the U.S., public access to the Internet is provided primarily by "Internet service providers" (ISPs) such as the Microsoft Network (MSN), America Online, and MCI, as well as scores of smaller providers serving various regional or metropolitan areas. In addition, many municipalities have established so-called "freenets" offering free or low-cost Internet access to local residents. Many users also have access through their employers or educational institutions.

It is worth emphasizing what the Internet is not. First, it is not a commercial service per se, although many commercial information services can be reached on the Internet. For example, the LEXIS/NEXIS information databases can be accessed via an Internet connection (assuming the user has previously established an account and obtained a password).

Second, the Internet is largely distinct from bulletin-board systems (BBSes). Historically, a BBS is a single freestanding computer reachable only by a direct telephone dialup (i.e., using a modem to call the BBS over a regular telephone line). BBSes commonly offer electronic mail, public discussion forums, and file archives. These last two are often devoted to one or more specialized areas of interest, sometimes including illegal activities. Because BBSes are often operated by hobbyists, user fees and access policies vary widely.

2. What the Internet Offers

The Internet offers a wide variety of resources for investigating (and, conversely, committing) criminal activity. The main facilities for locating, retrieving, or exchanging information are electronic mail, the World Wide Web, Usenet newsgroups, Internet Relay Chat (IRC) and similar chat room facilities, and FTP (file transfer protocol).

a. Electronic Mail (E-mail)

The most widely used Internet application, electronic mail allows a user to send information to any other person who has an Internet address. Addresses are conventionally written in the form *username@site*, where *site* is the name of the recipient's host computer (e.g., ibm.com) and *username* is a series of letters and/or numbers uniquely identifying the recipient.

Although most e-mail consists entirely of text, it is possible to send messages that contain one or more other types of documents such as graphic image files, digital audio, or executable programs.

Various electronic "mailing lists" (sometimes referred to as "listservs") exist for discussion of a wide variety of topics. Each member of the list (which may have as many as a thousand or more subscribers) has the ability to send e-mail to all the other members at the same time. Some mailing lists are moderated, meaning that the manager(s) of the list screens submissions for suitability before they are distributed to the members. The degree of public access also varies from list to list: some lists are invitation-only, others are open to all comers, and the traffic on some lists can even be read by nonsubscribers via archives kept on the World Wide Web (see below) or stored elsewhere.

b. The World Wide Web

The World Wide Web is a vast collection of electronic files residing on computers throughout the Internet. A Web page may contain text, graphics, video, or audio in any combination. It may also include hypertext links (also called "hot links" or "clickable links") to other Web pages anywhere on the Internet. Users visit web pages by means of a "browser" program (such as Netscape Navigator or Microsoft Internet Explorer) that allows them to move freely among Web pages by clicking the computer mouse on the available links. Although most pages on the Web are freely viewable by anyone with access to a browser, some sites require a password.

As the collective creation of thousands of web page contributors, the Web has no central index. However, a number of extensive commercial indexes (all updated regularly) enable users to perform keyword searches to locate sites concerning a given subject. Among the more popular search engines are Yahoo, Hotbot, Alta Vista, Infoseek, and Open Text, all of which are available on the Web itself.

c. Usenet Newsgroups and Similar Facilities

The Internet is also home to several thousand discussion groups known collectively as "Usenet". These discussion groups — also called "newsgroups" — allow users to post public messages (including replies to earlier messages) on a variety of topics. Interaction does not take place in real time: it more closely resembles a sequence of open letters than a multiparty telephone conversation.

Each newsgroup has a period-punctuated name that indicates its subject. For instance, talk.politics.misc is for miscellaneous political discussion. As with mailing lists, a newsgroup may be moderated, in which case postings are screened by one or more moderators for suitability. Even for moderated newsgroups, however, there is no way to restrict the group's readership, meaning that there are no private newsgroups. In theory, each newsgroup article is circulated to thousands of computers worldwide, and is therefore accessible to almost anyone on the Internet. Moreover, online archives (indexed on the World Wide Web) now exist for nearly all Usenet groups.

BBSes generally offer a comparable public discussion mechanism (which is the historical reason for calling such systems "bulletin boards"). Unlike Usenet articles, however, messages posted on a BBS are not typically distributed to other sites, and thus normally are accessible only to users of that system.

d. Internet Relay Chat (IRC) and Similar Communications Facilities

Internet Relay Chat (IRC) is a method for real-time discussion among multiple users. In each "channel" (discussion forum), participants are able to engage in the online equivalent of a party-line conversation, with response time limited only by one's typing speed. Discussion transcripts are not automatically created or stored unless an individual participant takes steps to do so. IRC channels, like mailing lists, may be either open to the public or invitation-only.

Note that IRC channels are used for discussions spanning multiple Internet sites. Many commercial services provide a similar facility for internal discussions among their members. On America Online, for example, these forums are called "chat rooms." As with IRC, these provider-specific discussion forums may generally be either open to the public or invitation-only.

In addition, services such as "ICQ" (I seek you) and "DCC" (direct channel chat) allow for private, one-to-one real-time chat activity.

e. File Transfer Protocol (FTP)

FTP is an older program used to transfer files (such as executable programs) directly from one computer system to another over the Internet. Its primary application is in retrieving files from publicly accessible archives; as a result, much of its usefulness has been taken over by the emergence of the World Wide Web. In fact, most Web browser programs are designed to be able to fetch documents from FTP archives.

f. Emerging Resources

As the Internet — especially the World Wide Web — continues to grow and evolve, new tools and resources for locating and retrieving information on the Internet are likely to emerge. For example, a number of software developers are working to create "intelligent agents," programs that can be customized by individual users to actively seek out information on one or more specified topics.

Several new "information push" services mark a step on the road toward full-fledged intelligent agents. At fixed intervals specified by the user, these services automatically access one or more remote host computers on the Internet and fetch information for viewing on the user's computer (sometimes as a screen saver display or as a "ticker" occupying part of the screen). The type of information retrieved is highly configurable: for example, a user may request regular updates on certain stock prices and market indexes, updates of a certain frequently changing Web page, or current wire service stories on a wide variety of topics.

Similarly, as bandwidth availability increases, the Internet will be used with increasing frequency to transmit real-time voice and video communications. Investigators are encouraged to consult with CCIPS in investigations involving emerging communications technologies, as some are likely to raise novel legal issues.

B. Illegal Online Activity

The vast majority of online users are law-abiding and responsible, and their activities — many of which involve the exercise of First Amendment rights of free speech and association — should not ordinarily be of concern to law enforcement agencies. At the same time, the Internet and other online environments are no more immune to criminal conduct than is the physical world. These media provide new opportunities for the coordination and commission of a variety of illegal acts. The following is an overview of the types of criminal methods and conduct investigators have encountered and are likely to encounter online.

Computers can play three different roles in criminal activity. First, a computer may be used as a weapon, where the criminal's objective is to steal information or services from, or cause damage to, the target system. Second, computers can be used as tools to facilitate an offense, such as electronic fraud. Finally, a computer may be used as a storage device for evidence or contraband. A single case may involve all three types of computer use.

1. Computer As Weapon

True "computer crime" involves using a computer to attack a victim computer, generally to acquire information stored on that target, to use the target system without payment (theft of service), or to damage the system. Most (but not all) such violations involve gaining unauthorized access to the target system (i.e., "hacking" into it).

a. Theft of Information

Offenses involving theft of information may take a variety of forms, depending on the nature of the system attacked. Sensitive information stored on law enforcement and military computers offers a tempting target to many parties, including subjects of criminal investigations, terrorist organizations, and foreign intelligence operatives.

Hackers also target non-governmental systems to obtain proprietary information or other valuable information. For example, in one case a hacker gained access to a hotel reservation system to steal credit card numbers. Other cases may fall into the broad category of intellectual property theft. This includes not only the theft of trade secrets, but also much more common offenses involving the unauthorized duplication of copyrighted materials, especially software programs.

Sometimes an attacker's motivation is to learn private information about another individual, whether as a means to an end (e.g., to extort money or to embarrass the victim through public disclosure) or simply to satisfy personal curiosity. Targets in this category include systems containing medical records, telephone customer records (such as call records or unlisted directory information), or consumer credit report information.

b. Theft of Services

A second class of violations involves gaining unauthorized access to a system for the purpose of obtaining unpaid-for services. For instance, an offender may use his computer to break into a telephone switching system (including a private system, such as a PBX) in order to steal long-distance calling services. (This type of telephone equipment manipulation is often referred to as "phone phreaking" or simply "phreaking.") In some cases, hackers have used the resources of compromised systems to perform intensive computational tasks such as cracking encrypted passwords stolen from other sites.

The most common theft-of-service offense is associated with the practice of "weaving," in which a hacker traverses multiple systems (and possibly multiple telecommunications

networks, such as the Internet or cellular and landline telephone networks) to conceal his true identity and location. In this scenario, the sole reason for breaking into a given computer may be to use it as a stepping-stone for attacks on other systems.

c. Damage to Systems

Even where an attacker's objective is not to obtain information from the target computer or to use it, he may have any of several other goals in mind. Perhaps most obvious is the case where the attacker intends to destroy or modify data important to the owner or user(s) of the victim system. Malicious attacks of this type are often carried out by disgruntled ex-employees seeking to retaliate for perceived unfair treatment. See, e.g., Sablan v. United States, 92 F.3d 865 (9th Cir. 1996) (shortly after dismissal, ex-employee of bank modified or deleted files on computer system).

A more insidious type of damage takes place in cases where the attacker compromises a system in furtherance of a larger scheme. The most well-known examples of this type of attack have involved telephone network computers. In one case, a hacker manipulated telephone switching equipment to guarantee that he would be the winning caller in several call-in contests held by local radio stations. The fruits of his scheme included two Porsches and $30,000 in cash.

Internet-connected computers are subject to similar types of attacks. Routers — computers that direct data packets traveling on the Internet — are analogous to telephone switches, and are thus tempting targets for skilled hackers interested in disrupting, or even rerouting, communications traffic on the network.

On many occasions, hackers have installed "sniffer" programs that illegally intercept user passwords during the login process. Because users often employ the same password on more than one computer system (contrary to prudent security practice), intercepting a user's password often provides a hacker easy access to other computer systems where that user has accounts. That access, in turn, greatly simplifies the hacker's task of compromising those other systems.

In the category of attacks known collectively as "denial of service," the objective is to disable the target system without necessarily gaining access to it. One technically straightforward method of accomplishing this objective is "mailbombing," the practice of sending large volumes of e-mail to a single site (or user account) in order to clog the mail server or even cause the target host to crash. Other methods, ranging from simply tying up incoming phone lines all the way to more sophisticated attacks using low-level data transmission protocols, may also be used to achieve the same end: rendering the target system unavailable for normal use.

2. Computer as Instrumentality of Traditional Offense

Computers may be an instrument in the perpetration of a traditional offense, such as a fraudulent marketing scheme. Frauds commonly attempted online include:

- **advance fee schemes**, in which the offender advertises the availability of goods or services and requires payment in advance. Only after paying do victims discover that the goods or services are defective, inferior, or nonexistent;

- **pyramid schemes and chain letters** essentially identical to those disseminated by postal mail. A conventional chain letter contains a list of names and addresses to whom recipients are urged to send money. Recipients are then expected to add their names to the list (often removing the topmost name to keep the number of participants constant) and to redistribute the updated letter; and

- **Ponzi schemes**, which differ from chain letters in that a Ponzi scheme promotes an allegedly lucrative business opportunity, often involving foreign currency exchange, precious metals trading, or other high-return investments. There is in fact no underlying business, and the perpetrator simply uses the money obtained from later investors to pay "profits" to earlier investors, thus giving the appearance of profitability and attracting additional victims.

Vehicles used to promote these frauds include the World Wide Web, Usenet (where solicitations are often posted indiscriminately to hundreds of newsgroups), Internet Relay Chat, and direct e-mail.

Online gambling operations, some of which may be illegal under 18 U.S.C. § 1084, have also become increasingly common. Made available most frequently on the Web, often from offshore, these operations range from simple lottery sites to sports betting operations or even full-blown "virtual casinos" offering a range of gaming activities. Aside from the potential illegality of the gambling transmissions themselves, there is also tremendous potential for fraud by the "house," as by rigging probabilities (in craps, for example), inspecting players' cards, or even refusing to pay stakes to winners. While most current operations obtain players' credit card numbers as a means of payment, the anticipated increase in the use of "digital cash" is likely to simplify online transactions and fuel growth in the gambling arena.

Online resources are also an inviting medium for would-be traffickers in obscene materials and child pornography. Cyberspace offers these individuals a number of advantages over the

physical world, including (a) the ability to be anonymous or to use a pseudonym instead of a real name, (b) the ease of locating and communicating with like-minded persons, and (c) the speed and ease of exchanging digitally stored images over long distances at minimal cost. Internet Relay Chat and/or chat rooms are common meeting grounds, with images distributed variously over Usenet, the Web, or via electronic mail. Individuals may also exploit the identity-concealing aspects of cyberspace to converse (and even arrange for in-person encounters) with intended victims.

Additionally, criminals illegally use electronic distribution methods to reproduce materials protected by copyright. Online copyright piracy is an ever-increasing threat to creators of software, music, books, and movies.

While these crimes are those most commonly encountered in the online realm, it is worth emphasizing that online facilities may be used in the furtherance of a broad range of traditional criminal activity. Electronic mail and chat sessions can be used to plan or coordinate almost any type of unlawful act, or even to communicate threats or extortionate demands to victims. As robust encryption methods become more widespread, criminals can be expected to use this technology to evade detection in the planning and execution of their illegal activities.

3. Computers as Storage Devices

The third role a computer can play in criminal activity is that of passive storage medium. In many cases, this use will be ancillary to the system's other role as the victim of an intrusion.

For example, after compromising a system a hacker will often create a special directory for storing files. These files may include hacking software tools, password files (or password lists) for other sites, or lists of stolen credit card numbers. By hiding these types of information on a remote system, a hacker makes it more difficult to tie these articles to him in the event he comes under law enforcement scrutiny.

Hackers may also use these storage locations as "dead drops" or even clearinghouses for distribution of password lists, credit card and calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software).

APPENDIX B
ONLINE INVESTIGATIONS WORKING GROUP: AGENCY POINTS OF CONTACT

Main Justice

David Green (Co-chair)
Deputy Chief
Computer Crime & Intellectual Property Section
Criminal Division

Tony Whitledge (Co-chair)
Senior Trial Attorney
Tax Division

Scott Charney
Chief
Computer Crime & Intellectual Property Section
Criminal Division

Marty Stansell-Gamm
Principal Deputy Chief
Computer Crime & Intellectual Property Section
Criminal Division

Mark Eckenwiler
Trial Attorney
Computer Crime & Intellectual Property Section
Criminal Division

Thomas N. Burrows
Deputy Chief
Child Exploitation & Obscenity Section
Criminal Division

Hemanshu Nigam
Trial Attorney
Child Exploitation & Obscenity Section
Criminal Division

Terri Shubert
Trial Attorney
Office of International Affairs
Criminal Division

Robert De La Cruz
Trial Attorney
Terrorism and Violent Crimes Section
Criminal Division

Julia Stiller
Trial Attorney
Organized Crime & Racketeering Section
Criminal Division

Paul Morris
Counsel
Office of Policy Development

Mark Greenberg
Deputy Assistant Attorney General
Office of Policy Development

Jessica Ginsburg
Deputy Chief
Criminal Section
Civil Rights Division

Marty Lederman
Attorney Advisor
Office of Legal Counsel

John T. Webb
Assistant Chief
Wildlife & Marine Resources Section
Environment and Natural Resources Division

Kenneth W. Gaul
Trial Attorney
Computers and Finance Section
Antitrust Division

Michael Bromwich
Inspector General

U.S. Attorney's Offices

Stephen Heymann
Deputy Chief
Criminal Division
District of Massachusetts

John McEnany
Associate U.S. Attorney
Southern District of New York

Randy Chartash
Assistant U.S. Attorney
Northern District of Georgia

Joseph Koehler
Counsel to the Director
Executive Office of United States Attorneys

Federal Bureau of Investigation

Larry Parkinson
General Counsel

Flora Francis
Assistant General Counsel

Steve Chabinsky
Assistant General Counsel of the
Office of General Counsel
National Infrastructure Protection Center

Rich Ress, S.S.A.
National Computer Crime Squad
Washington Field Office

Ed Stroz, S.S.A.
National Computer Crime Squad
New York Field Office

Kenneth M. Geide
Section Chief
National Infrastructure Protection Center

Doris Gardner
Supervisory Special Agent
Computer Investigations Unit
National Infrastructure Protection Center

Karen Spangenberg, Chief
Financial Institution Fraud Unit

Mike Morris, S.A.
Dallas Field Office

Other D.O.J. Agencies

Mike Phelan
Acting Chief
Computer Forensics Unit
Drug Enforcement Administration

Richard L. Brown
Electronics Engineer
Drug Enforcement Administration

Darryl Kelley
Supervisory Inspector
United States Marshal's Service

Christopher Pohl
Supervisory Special Agent
Immigration and Naturalization Service

Treasury Department

Karen Wehner
Deputy Assistant Secretary for Enforcement

Scott Everett
Policy Liaison
Mark James
Office of Enforcement Policy

Richard Mendrop
Director
Computer Investigative Specialists Program
IRS-DI

Andrew Fried
Assistant Special Agent in Charge
Computer Forensics Division
Tax Administration
Inspector General's Office

Richard Delmar
Technical Assistant
Office of Chief Counsel
Internal Revenue Service

Tom Dougherty
Senior Counsel
U.S. Secret Service

William E. Clancy
Special Agent in Charge
Office of Chief Counsel
U.S. Secret Service

Mary Riley
Special Agent in Charge
Electronic Crimes Branch
U.S. Secret Service

John Minsek
Computer Recovery Specialist
Forensic Science Laboratory
Bureau of Alcohol, Tobacco & Firearms

Deputy Chief

Intelligence Division
Bureau of Alcohol, Tobacco & Firearms

Abby Roth
Staff Attorney
Bureau of Alcohol, Tobacco & Firearms

Jerry Burg, S.S.A.
U.S. Customs Service

Kevin Manson
Senior Instructor
Federal Law Enforcement Training Center

Stephen Kroll
Legal Counsel
Financial Crimes Enforcement Center

Other Federal Agencies

Richard Shiffrin
Deputy General Counsel for Intelligence
Department of Defense

Major Stanley Smith
Judge Advocate General Corps
Air Force Office of Special Investigations

Tom Talleur
Advanced Technology Programs Executive
Computer Crimes Division
Office of the Inspector General
NASA

John J. Rooney
Criminal Investigator
Office of Criminal Investigations

Food and Drug Administration

Sam Guttman
Manager, Digital Evidence Unit
U.S. Postal Service