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.

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

---

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

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 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

---

[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.

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]

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

---

[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.

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 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

---

[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.

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 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.

---

[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.

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 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]

---

[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 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.

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]

---

[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.**

[24] [redacted]

b2, b7E

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 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

b2
b7E

b2
b7E

b2
b7E

b2
b7E

b2
b7E

b2
b7E

b2
b7E