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

(continued...)

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. b2, b7E

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 cooperating witness may communicate electronically with others and log those

[29](...continued) 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.

[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.

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

b2

b7E

b2
b7E

b2
b7E

b2
b7E

b2, b7E

PART III: OTHER ISSUES

PRINCIPLE 10

ONLINE ACTIVITY BY AGENTS DURING PERSONAL TIME

While not on duty, an agent is generally free to engage in personal online pursuits. If, however, the agent's 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 witnesses and informants from Denmark as from Des Moines. Moreover, because it is easy to

[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.

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.

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

[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.

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 dó 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** b2, b7E 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 <u>not</u>. First, it is not a commercial service <u>per se</u>, 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 (<u>i.e.</u>, 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. <u>Electronic Mail (E-mail)</u>

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 (<u>e.g.</u>, 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).