Chapter 4
Special Considerations

A. Jurisdiction

1. Interstate Commerce or Communication Requirement

Several of the statutes discussed in this manual require an interstate or foreign jurisdictional hook. *See, e.g.,* 18 U.S.C. § 1029(a) (prohibiting access device fraud "if the offense affects interstate or foreign commerce"); 18 U.S.C. § 2510(12) (defining "electronic communication" to mean any "transfer of signs, signals, writing, images, sounds, data, or intelligence ... that affects interstate or foreign commerce"). Failure to establish the "interstate" basis for federal jurisdiction can lead to dismissal or acquittal. *See United States v. Jones*, 580 F.2d 219 (6th Cir. 1978) (affirming judgment of acquittal in wiretap case where government failed to offer evidence that telephone company provided facilities for the transmission of interstate or foreign communications).

Many of the charges in 18 U.S.C. § 1030 prohibit unlawful access of a "protected computer," which includes a computer used in "interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). In most cases, demonstrating that a computer was connected to the Internet will satisfy this requirement. Section 1030(a)(2)(C) requires a more particular nexus—the unlawful conduct itself must involve an interstate or foreign communication. *See* 18 U.S.C. § 1030(a)(2)(C). Prosecutors should be prepared to offer evidence that the conduct in fact traversed state lines. Useful evidence might include testimony as to the geographic location of computer servers. Bear in mind that even a "local" provider may utilize communication facilities in another state.

2. Extraterritoriality

Absent evidence of a contrary intent, the laws of the United States are presumed *not* to have extraterritorial application. *See United States v. Cotten*, 471 F.2d 744, 750 (9th Cir. 1973). This presumption against extraterritoriality may be overcome by showing "clear evidence of congressional intent to apply a statute beyond our borders." *United States v. Gatlin*, 216 F.3d 207, 211 (2d Cir. 2000) (internal quotations omitted). "Congress has the authority to enforce its

laws beyond the territorial boundaries of the United States. Whether Congress has in fact exercised that authority in [a particular case] is a matter of statutory construction." *Equal Employment Opportunity Comm. v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991) (internal citations omitted).

In 2001, as part of the USA PATRIOT Act, Congress revised both sections 1029 and 1030 to explicitly provide for extraterritorial jurisdiction in certain cases. The USA PATRIOT Act added the following language to section 1029:

> (h) Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if—
>
> > (1) the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and
> >
> > (2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.

18 U.S.C. § 1029(h).

The Act also amended section 1030(e)(2)(B) to specifically include a computer "which is used in interstate or foreign commerce, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." *See* 18 U.S.C. § 1030(e)(2)(B). Even prior to the 2001 amendment, however, at least one court held that the plain language of 18 U.S.C. § 1030 was a clear manifestation of congressional intent to apply that section extraterritorially. *See United States v. Ivanov*, 175 F. Supp. 2d 367, 374-75 (D. Conn. 2001).

Extraterritorial jurisdiction can be found not only on the basis of specific congressional intent, but also on the basis of intended and actual detrimental effects within the United States. "The intent to cause effects within the United States ... makes it reasonable to apply to persons outside United States territory a statute which is not extraterritorial in scope." *United States v. Muench*, 694

F.2d 28, 33 (2d Cir. 1982). "It has long been a commonplace of criminal liability that a person may be charged in the place where the evil results, though he is beyond the jurisdiction when he starts the train of events of which that evil is the fruit." *United States v. Steinberg*, 62 F.2d 77, 78 (2d Cir. 1932).

Other sources of extraterritorial jurisdiction may include 18 U.S.C. § 7, which defines the special maritime and territorial jurisdiction of the United States, and 18 U.S.C. §§ 3261-3267, which govern criminal offenses committed outside of the United States by members of the military and persons employed by or accompanying them.

B. Venue

1. Background

Venue is governed by a combination of constitutional provisions, statutes, and rules. *See* 2 Charles Alan Wright, *Federal Practice & Procedure* § 301 (3d ed. 2000). The Constitution mandates that trial be held in the state and district where the crime was committed. *See* U.S. Const. art. III, § 2, cl. 3; U.S. Const. amend. VI. This principle is implemented by Federal Rule of Criminal Procedure 18, which states in full: "Unless a statute or these rules permit otherwise, the government must prosecute an offense in a district where the offense was committed. The court must set the place of trial within the district with due regard for the convenience of the defendant and the witnesses, and the prompt administration of justice." Fed. R. Crim. P. 18. However, the Constitution and Rule 18 still leave many questions unanswered in many network crime cases, such as how to define where an offense has been "committed" or how to deal with crimes committed in multiple states or countries.

Note that when a defendant is charged with more than one count, venue must be proper with respect to each count. *See United States v. Salinas*, 373 F.3d 161, 164 (1st Cir. 2004) ("The criminal law does not recognize the concept of supplemental venue"). If no single district has proper venue for all potential counts, prosecutors can either charge the defendant in multiple districts and seek transfer to a single district or bring all charges in one district and seek a waiver from the defendant. Rule 20 of the Federal Rules of Criminal Procedure allows transfer of prosecution for purposes of entering a guilty plea, from the district where the indictment is pending to the district where the defendant is arrested, held, or present. Similarly, Rule 21 allows a court to transfer a prosecution for trial, upon the defendant's motion, to another district for the

convenience of the parties and witnesses. Note, however, that both rules require the explicit consent and cooperation of the defendant. A defendant may also waive any objections to improper venue, either explicitly or by failing to object when the defect in venue is clear. *See United States v. Roberts*, 308 F.3d 1147, 1151-52 (11th Cir. 2002); *United States v. Novak*, 443 F.3d 150, 161 (2d Cir. 2006).

2. Locations of Network Crimes

Applying the principles of venue to network crimes is not always a straightforward endeavor. As described above, the central inquiry in venue analysis is determining where the crime was committed. Yet, "in today's wired world of telecommunication and technology, it is often difficult to determine exactly where a crime was committed, since different elements may be widely scattered in both time and space, and those elements may not coincide with the accused's actual presence." *United States v. Saavedra*, 223 F.3d 85, 86 (2d Cir. 2000); *see United States v. Rowe*, 414 F.3d 271 (2d Cir. 2005) (finding venue in district where agent connected to Internet, entered chat room, and saw defendant's posting in child porn case).

None of the intrusion crimes discussed in Chapter 1 contains specific venue provisions. Moreover, few reported cases address venue for these crimes. *See, e.g., United States v. Ryan*, 894 F.2d 355 (10th Cir. 2000) (noting that 18 U.S.C. § 1029 does not specify venue); *Berger v. King World Productions, Inc.*, 732 F. Supp. 766 (E.D. Mich. 1990) (examining venue under 28 U.S.C. § 1391(b) in a civil suit arising pursuant to 18 U.S.C. § 2511).

Multidistrict offenses "may be ... prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a) Note that only the "essential conduct elements" of a crime qualify. *United States v. Rodriguez-Moreno*, 526 U.S. 275, 280 (1999). For instance, section 1030(a)(2)(C) prohibits intentionally accessing a computer without or in excess of authorization, and thereby obtaining information from any protected computer if the conduct involved an interstate or foreign communication. The two essential conduct elements in section 1030(a)(2)(C) are "accessing" a computer and "obtaining" information. Thus, it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access *and* where the information is obtained.

The exact location of each event—the "accessing" and the "obtaining"—may not always be easily determined.

Example: *An intruder located in California uses communications that pass through a router in Arizona to break into a network in Illinois, and then uses those network connections to obtain information from a server in Kentucky.*

The intruder initiated access in California, the router in Arizona enabled that access, but arguably the intruder did not achieve access until reaching the network in Illinois. Of course, one could also argue that access did not occur until the intruder reached the server in Kentucky where the information was located. Likewise, the intruder may have obtained the information in Kentucky, or he may not have obtained the information until it reached him in the district where he was located, in this case, California.

This example illustrates an offense governed by 18 U.S.C. § 3237(a). Under any of the options discussed above, the appropriate venue would seem to include both of the endpoints—that is, the district in which the offender is located (California) and the district in which the information is located (Kentucky). It is likely that venue is also proper at some, if not all, of the points in between, since venue may lie "in any district in which [a continuing] offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Under this section, the "accessing" and "obtaining" were arguably continued in Arizona and Illinois. Certainly, venue seems proper in Illinois where the intruder broke into the network. Whether it can be said that the intruder committed a crime in Arizona is less clear.

Prosecutors looking to fix venue in the locale where communications simply pass through, as in the case of the router in Arizona, should look closely at the facts to determine whether venue in that district would satisfy the framework discussed above.[1] The case for "pass through" venue may be stronger where transmission of the communications themselves constitutes the criminal offense (e.g., when a threatening email is sent in violation of 18 U.S.C. § 1030(a)(7)) and the path of transmission is certain (e.g., when an AOL subscriber's email is sent through a mail server in Virginia).[2] By contrast, in cases where the path of transmission is unpredictable, a court may find it difficult to conclude that a crime was committed in a district merely because packets of information

[1] As a practical matter, it may be difficult to prove that the intruder's communications traveled through a particular router in a particular geographic location.

[2] The type of "pass through" venue described in this paragraph does not cover the situation where the "pass through" computer itself is hacked. In that case, venue would likely be proper based on the hack rather than the "pass through."

happened to travel through that district. *Cf. Ashcroft v. ACLU*, 535 U.S. 564, 602 (2002) (Kennedy, J., concurring) ("In the context of COPA, it seems likely that venue would be proper where the material originates or where it is viewed. Whether it may be said that a website moves "through" other venues in between is less certain.").

Federal prosecutors should also take note of the Department of Justice's policies for wire and mail fraud, which may be analogous. For wire fraud, section 967 of the Department's Criminal Resource Manual provides that prosecutions "may be instituted in any district in which an interstate or foreign transmission was issued or terminated." *Crim. Resource Manual* § 967. Although the text of section 967 refers only to the place of issuance or termination, the case cited in support of that proposition, *United States v. Goldberg*, 830 F.2d 459, 465 (3d Cir. 1987), relies on 18 U.S.C. § 3237(a), which also includes the place where the conduct continued, thus leaving open the door to "pass through" venue. In the case of mail fraud, section 9-43.300 of the U.S. Attorneys' Manual "opposes mail fraud venue based solely on the mail matter passing through a jurisdiction." USAM 9-43.300; see also Crim. Resource Manual § 966.

In some cases, venue might also lie in the district where the effects of the crime are felt. The Supreme Court has not faced that question directly. *See United States v. Rodriguez-Moreno*, 526 U.S. 275, 279 n.2 (1999) ("The Government argues that venue also may permissibly be based upon the effects of a defendant's conduct in a district other than the one in which the defendant performs the acts constituting the offense. Because this case only concerns the *locus delicti*, we express no opinion as to whether the Government's assertion is correct."). However, other courts that have examined the issue have concluded that venue may lie "where the effects of the defendant's conduct are felt, but only when Congress has defined the essential conduct elements in terms of those effects." *United States v. Bowens*, 224 F.3d 302, 314 (4th Cir. 2000), *cert. denied,* 532 U.S. 944 (2001). Thus, charges under provisions like 18 U.S.C. § 1030(a)(5) may be brought where the effects are felt because those charges are defined in terms of "damage," even if the bulk of network crimes may not be prosecuted in a district simply because the effects of the crime are felt there. Prosecutors seeking to establish venue by this method are encouraged to contact CCIPS at (202) 514-1026.

C. Statute of Limitations

With one exception, the Computer Fraud and Abuse Act subsections discussed in Chapter 1 do not contain a specific statute of limitations for criminal prosecutions. *But see* 18 U.S.C. § 1030(g) (requiring *civil* actions to be brought "within 2 years of the date of the act complained of or the date of the discovery of the damage"); 18 U.S.C. § 2707(f) (creating two-year statute of limitations for *civil* actions); 18 U.S.C. § 2520(e) (providing that any *civil* action "may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation").

In the absence of a specific statute of limitations, the default federal limitations period of five years applies. *See* 18 U.S.C. § 3282. The exception to the five-year default limit is 18 U.S.C. § 1030(a)(1), which is now included in the list of offenses in 18 U.S.C. § 2332b(g)(5)(B), which offenses are incorporated into 18 U.S.C. § 3286. The statute of limitation for those crimes is extended to eight years, and is totally eliminated for offenses that resulted in, or created a foreseeable risk of, death or serious bodily injury to another person.

For cases involving evidence located in a foreign country, prosecutors can request that the court before which an investigative grand jury is impaneled suspend the statute of limitations, if the court finds by a preponderance of the evidence: (1) that an official request has been made for such evidence; and (2) that it reasonably appears, or reasonably appeared at the time the request was made, that such evidence is, or was, in such foreign country. *See* 18 U.S.C. § 3292. Note that such requests may be made *ex parte*, must be made before return of an indictment, and must bear sufficient indicia of reliability, such as by sworn or verified application. *See United States v. Trainor*, 376 F.3d 1325 (11th Cir. 2004).

D. Juveniles[3]

In the 1983 movie *War Games*, Matthew Broderick and Ally Sheedy play high school students who inadvertently access the NORAD computer network, thinking that they are merely playing a "war game" with the computers. As

[3] This section is adapted from an article written by Joseph V. DeMarco, Assistant United States Attorney for the Southern District of New York, and published in the May 2001 U.S. Attorneys' Bulletin. Mr. DeMarco currently serves as a Computer Hacking and Intellectual Property Coordinator in the Southern District and formerly served as a detailee to CCIPS.

a consequence, Broderick and Sheedy come Hollywood-close to initiating a nuclear exchange between the United States and the Soviet Union. In order to accomplish this hack, Broderick configures his computer's modem to automatically dial random telephone numbers in the city where the computers he hopes to break into are located. When Sheedy asks Broderick how he pays for all the telephone calls, Broderick coyly tells her that "there are ways around" paying for the phone service. Sheedy asks: "Isn't that a crime?" Broderick replies: "Not if you are under eighteen."

This section demonstrates why Broderick was wrong. Federal prosecutors can bring juvenile offenders to justice, but must understand the applicable provisions of the criminal code. Specifically, the Federal Juvenile Delinquency Act (FJDA), 18 U.S.C. §§ 5031-5042, governs the criminal prosecution and the delinquent adjudication of minors in federal court.

While a complete analysis of the FJDA is beyond the scope of this manual, certain of its provisions merit discussion because proceedings against juveniles in federal court differ in significant respects from the prosecution of adults. The FJDA creates a unique procedure for delinquency proceedings against juveniles—a process that is quasi-criminal and quasi-civil in nature, replete with its own procedural complexities and particular rules.

As a threshold matter, it is important to note that a juvenile proceeding is not the same as a criminal prosecution. Rather, it is a proceeding in which the issue to be determined is whether the minor is a "juvenile delinquent" as a matter of status, not whether he or she is guilty of committing a crime. Thus, a finding against the juvenile does not result in a criminal conviction; instead, it results in a finding of "delinquency." Indeed, the juvenile proceeding is specifically designed to *lessen* the amount of stigma that attaches to the act of delinquency compared to a criminal conviction, and to emphasize the rehabilitation, rather than punishment, of the juvenile. *See, e.g., United States v. Hill*, 538 F.2d 1072, 1074 (4th Cir. 1976). With that background in mind, several aspects of the FJDA are examined below.

1. Definition of Juvenile

Under the FJDA, a "juvenile" is a person who has not yet reached the age of eighteen at the time of the commission of the offense *and* is under twenty-one as of the time of the filing of formal juvenile charges. *See* 18 U.S.C. § 5031. Thus, a person who committed the offense before his eighteenth birthday, but is over twenty-one on the date formal charges are filed, may be prosecuted as

an adult. The juvenile delinquency proceedings would not apply at all in that case. This is true even where the government could have charged the juvenile prior to his twenty-first birthday, but did not. *See In re Jack Glenn Martin*, 788 F.2d 696, 698 (11th Cir. 1986) (holding that determinative date is date of filing of formal indictment or information; fact that government could have brought charges against defendant prior to his twenty-first birthday held to be "irrelevant"); *see also United States v. Hoo*, 825 F.2d 667 (2d Cir. 1987) (holding that absent improper delay by government, age at time of filing of formal charges determines whether FJDA applies).

2. Federal Jurisdiction

As is true in the case of adults, not every criminal act committed by a juvenile violates federal law. Only where Congress has determined that a particular federal interest is at stake, and has passed appropriate legislation, can a federal criminal prosecution go forward. In general, under the FJDA, there are three situations where federal delinquency jurisdiction over a juvenile exists. The first is where the state court lacks jurisdiction or refuses to assume jurisdiction. *See* 18 U.S.C. § 5032. The second is where the state does not have available programs and services adequate for the needs of juveniles. *See id.* The third is where the crime is a federal felony crime of violence or one of several enumerated federal offenses (principally relating to narcotics and firearm offenses), and a substantial federal interest exists to warrant exercise of federal jurisdiction. *See id.*

No State Statute or State Refuses Jurisdiction

This first basis for federal jurisdiction will be the most frequently used basis in the context of juvenile delinquency involving computers. It encompasses situations where a state has no law criminalizing the specific conduct, or does have a law, but for whatever reason, indicates that it will not pursue proceedings under its law against the minor. With regard to the former, although many states have enacted laws analogous to statutes such as the federal network crime statute (18 U.S.C. § 1030), the electronic wiretap statute (18 U.S.C. § 2511), and the access device fraud statute (18 U.S.C. § 1029), some states do not have laws under which the acts in question can be prosecuted. In these cases, the FJDA nevertheless allows the juvenile to be held accountable for his or her act of delinquency under federal law.

More commonly, however, a state will have a statute that does cover the crime in question, *see, e.g.,* N.Y. Penal Law § 156.10 (computer trespass);

§ 156.27 (computer tampering in the first degree); § 250.05 (intercepting or accessing electronic communications), but will be unwilling to assume jurisdiction over the juvenile, perhaps because of a shortage of resources, or a dearth of technical or prosecutorial expertise. In such cases, upon certification by the United States Attorney that pertinent state officials do not wish to proceed against the juvenile, the federal government may assume jurisdiction. *See* 18 U.S.C. § 5032.

In the context of intrusion crimes, certain offenses committed by juveniles may amount to crimes in multiple states. A crippling denial of service attack or the transmission of a computer virus can generate victims in numerous jurisdictions. The FJDA, however, does not appear to require the government to certify that each and every state that could potentially assert jurisdiction is unwilling to assume that jurisdiction. The FJDA merely requires that the "juvenile court or other appropriate court of *a State* does not have jurisdiction or refuses to assume jurisdiction over [the] juvenile." 18 U.S.C. § 5032 (emphasis added). Typically, the pertinent state will be the state contemplating proceedings against the minor which, in practice, will often be the state in which the federal prosecutor investigating the case sits. Of course, because federal criminal proceedings can often preclude state criminal proceedings under state double jeopardy principles, federal prosecutors faced with multistate cases should consult with prosecutors from all affected states in order to determine what, if any, effect a federal juvenile proceeding may have on a state's proceedings. Consultation is also warranted because certain states may provide for treatment of the juvenile as an adult more easily than the transfer provisions of the FJDA (discussed below).

The State Has No Programs or Inadequate Programs

This second basis for federal jurisdiction arises infrequently, as most states do in fact have programs and facilities that provide for the adjudication, detention, and rehabilitation of minors. However, in the event that state officials were, for any reason, unable to address the needs of a juvenile, this exception would apply.

Enumerated Crimes and Crimes of Violence

The FJDA sets forth certain federal crimes for which jurisdiction is deemed to exist where there is a substantial federal interest. The enumerated offenses are controlled substance offenses under 21 U.S.C. §§ 841, 952(a), 953, 955, 959, 960(b)(1), (2), or (3), as well as firearms-related offenses under 18 U.S.C.

§§ 922(x), 924(b), (g), or (h). While these offenses typically do not apply to computer intrusion cases, the FJDA also permits jurisdiction in cases of "crimes of violence" that are punishable as felonies. *See* 18 U.S.C. § 5032. Although the FJDA itself does not define "crimes of violence," 18 U.S.C. § 16 states that such offenses "ha[ve] as an element the use, attempted use, or threatened use of physical force against the person or property of another." 18 U.S.C. § 16. "Crimes of violence" also include any offense "that is a felony and that, by its nature, involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense." 18 U.S.C. § 16.

Most of the intrusion offenses discussed in this manual do not involve physical force. However, several statutes may implicate this basis for jurisdiction in the context of computer-related crime, including 18 U.S.C. § 875(b) (transmission in interstate or foreign commerce of extortionate threats to injure another person), 18 U.S.C. § 1951(a) and (b)(2) (interference with commerce by extortion or threats of physical violence), and 18 U.S.C. § 844(e) (transmission of bomb threats).

Prosecutors relying on this third basis for jurisdiction should keep in mind that their certification must not only set forth a federal felony crime of violence, but must also certify that a substantial federal interest in the case or offense justifies federal jurisdiction. Eight of the nine circuits that have addressed the issue have held that the United States Attorney's certification of a substantial federal interest is not subject to appellate review for factual accuracy; only the Fourth Circuit has held otherwise. *See United States v. John Doe*, 226 F.3d 672, 676-78 (6th Cir. 2000) (collecting cases).

Where the federal government is the victim of a crime, the federal interest is apparent. Yet, even when the government is not the victim, federal interests often exist because network crimes affect critical infrastructures (e.g., telecommunications systems), industries or technologies significant to the nation's economy (e.g., aerospace, computer software), or are committed by criminals operating in multiple states and/or foreign countries. In these important and hard-to-enforce-locally situations, federal jurisdiction may be particularly appropriate.

3. Delinquency Proceedings

Assuming that federal juvenile jurisdiction exists, prosecutors bringing such actions will typically commence the action with the filing, under seal,

of a juvenile information and the jurisdictional certification. *See* 18 U.S.C. § 5032. It is important to note that the certification must be signed by the United States Attorney personally, and a copy of the pertinent memorandum delegating authority from the Assistant Attorney General to the United States Attorney to sign the certification should be attached to the submission. *See id.* (requiring certification of "the Attorney General").

A juvenile has no Fifth Amendment right to have his or her case presented to a grand jury, nor does the juvenile have the right to a trial by jury. *See, e.g., United States v. Hill*, 538 F.2d 1072, 1075-76 (4th Cir. 1976); *United States v. Indian Boy*, 565 F.2d 585, 595 (9th Cir. 1975). Instead, the "guilt" phase of a delinquency proceeding is essentially conducted as a bench trial. In that trial, the government must prove that the juvenile has committed the act of delinquency beyond a reasonable doubt, and the juvenile has many of the same rights as a criminal defendant. These include: (1) the right to notice of the charges; (2) the right to counsel; (3) the right to confront and cross-examine witnesses; and (4) the privilege against self-incrimination. *See Hill*, 538 F.2d at 1075 n.3 (collecting cases). Moreover, in the delinquency proceeding, the Federal Rules of Criminal Procedure apply to the extent that their application is not inconsistent with any provision of the FJDA. *See* Fed. R. Crim. P. 1(a)(5)(D); *see also* 3B Charles Alan Wright et al., *Federal Practice & Procedure* § 873 (3d ed. 2004). The Federal Rules of Evidence likewise apply to the delinquency proceeding, *see* F.R.E. 101, 1101, although courts have held them inapplicable to transfer proceedings (discussed below). *See Government of the Virgin Islands in the Interest of A.M., a Minor*, 34 F.3d 153, 160-62 (3d Cir. 1994) (collecting cases).

The Act also affords juveniles special protections not ordinarily applicable to adult defendants. Most notably, the juvenile's identity is protected from public disclosure. *See* 18 U.S.C. § 5038 (provisions concerning sealing and safeguarding of records generated and maintained in juvenile proceedings). Thus, court filings should refer to the juvenile by his or her initials and not by name, and routine booking photographs and fingerprints should not be made or kept. Moreover, when a juvenile is taken into custody for an alleged act of delinquency, the juvenile must be informed of his or her legal rights "in language comprehensible to [the] juvenile," 18 U.S.C. § 5033, and the juvenile's parent, guardian, or custodian must be notified immediately of the juvenile's arrest, the nature of the charges, and the juvenile's rights. *Id.* Upon arrest, the juvenile may not be detained for longer than a reasonable period

of time before being brought before a magistrate. *Id.* When brought before a magistrate, the juvenile must be released to his or her parents or guardian upon their promise to bring the juvenile to court for future appearances, unless the magistrate determines that the detention of the juvenile is required to secure his or her appearance before the court, or to insure the juvenile's safety or the safety of others. *See* 18 U.S.C. § 5034. At no time may a juvenile who is under twenty-one years of age and charged with an act of delinquency or adjudicated delinquent be housed in a facility where he or she would have regular contact with incarcerated adults. *See* 18 U.S.C. §§ 5035, 5039. Under the FJDA, a juvenile has a right to counsel at all critical stages of the proceeding, and the FJDA authorizes the appointment of counsel where the juvenile's parents or guardian cannot afford to retain counsel. *See* 18 U.S.C. § 5034.

4. Transfers to Adult Criminal Proceedings

As noted above, under certain circumstances, a juvenile's case may be transferred to adult status and the juvenile can be tried as an adult. In these situations, the case proceeds as any criminal case would, with the exception that a juvenile under eighteen who is transferred to adult status may *not* be housed with adults at any time pretrial or post trial. *See* 18 U.S.C. §§ 5035, 5039. A juvenile may transfer to adult status by waiving his juvenile status, upon written request and advice of counsel. *See* 18 U.S.C. § 5032. In addition, the FJDA creates two forms of transfer which do not depend on waiver: discretionary transfer and mandatory transfer.

As the name implies, discretionary transfer is an option available, upon motion by the government, in certain types of cases where the juvenile is fifteen or older at the time of the commission of the act of delinquency. *See* 18 U.S.C. § 5032. Such transfer is available in cases involving felony crimes of violence and other enumerated crimes. Under the FJDA, a court must consider six factors in determining whether it is in the interest of justice to grant the government's motion for discretionary transfer: (1) the age and social background of the juvenile; (2) the nature of the alleged offense, including the juvenile's leadership role in a criminal organization; (3) the nature and extent of the juvenile's prior delinquency record; (4) the juvenile's present intellectual development and psychological maturity; (5) the juvenile's response to past treatment efforts and the nature of those efforts; and (6) the availability of programs to treat the juvenile's behavioral problems. *See* 18 U.S.C. § 5032. In the context of typical computer crimes committed by juveniles, several of the factors will often counsel in favor of transfer to adult status: many computer

delinquents come from middle-class or affluent backgrounds; many commit their exploits with the assistance of other delinquents; and many are extremely intelligent. Moreover, many of the most sophisticated computer criminals are barely under the age of eighteen and, as such nearly-adult offenders, may merit punishment as adults.

Mandatory transfer is much more circumscribed than discretionary transfer; it is limited to either certain enumerated offenses (e.g., arson), which typically are not applicable in network crime prosecutions, or to violent felonies directed against other persons. *See* 18 U.S.C. § 5032. Mandatory transfer is also limited to offenses committed by juveniles sixteen or older who have a prior criminal conviction or juvenile delinquency adjudication for which they could be subject to mandatory or discretionary transfer. As a practical matter, therefore, in the area of network crimes, the majority of proceedings begun as juvenile proceedings will likely remain as such, and will not be transferred to adult prosecutions.

Federal prosecutors who are considering filing a motion to transfer a juvenile proceeding to adult criminal court should notify the Domestic Security Section of the Criminal Division at (202) 616-5731.

5. Sentencing and Detention

Under the FJDA, a court has several options in sentencing a juvenile adjudged to be delinquent. The court may suspend the finding of delinquency, order restitution, place the juvenile on probation, or order that the juvenile be detained. *See* 18 U.S.C. § 5037(a). In cases where detention is ordered, such detention can never be longer than the period of detention the juvenile would have received had he or she been an adult. *See* 18 U.S.C. § 5037(b). Accordingly, the Sentencing Guidelines, although not controlling, must be consulted. *See* U.S.S.G. § 1B1.12; *see also United States v. R.L.C.*, 503 U.S. 291, 307 n.7 (1992). Finally, if the disposition hearing is before the juvenile's eighteenth birthday, he or she may be committed to official detention until his or her twenty-first birthday or the length of time he or she would have received as an adult under the Sentencing Guidelines, whichever term is less. If the juvenile is between eighteen and twenty-one at the time of the disposition, he or she may be detained for a maximum term of three or five years (depending on the type of felony relevant to the proceeding), but in no event can he or she be detained longer than the comparable adult sentence under the Guidelines. *See* 18 U.S.C. § 5037(b), (c).

6. Other Considerations

As demonstrated above, federal delinquency proceedings are unique from a legal point of view, and prosecutors initiating such proceedings would do well to consult closely with the provisions of the United States Attorneys' Manual concerning delinquency proceedings, *see* USAM § 9-8.00, as well as the Domestic Security Section, which serves as the Department's expert in this field. Prosecutors should also familiarize themselves with the legal issues typically litigated in this area in order to avoid common pitfalls. *See, e.g.*, Jean M. Radler, Annotation, *Treatment Under Federal Juvenile Delinquency Act (18 U.S.C. §§ 5031-5042) of Juvenile Alleged to Have Violated Law of United States*, 137 A.L.R. Fed. 481 (1997).

In addition to the novel nature of the proceedings themselves, crimes committed by juveniles pose unique investigative challenges. For example, common investigative techniques such as undercover operations and the use of cooperators and informants can raise difficult issues rarely present in the investigation of adults. Indeed, a seemingly routine post-arrest interview may raise special issues of consent and voluntariness when the arrestee is a juvenile. *Compare United States v. John Doe*, 226 F.3d 672 (6th Cir. 2000) (affirming district court's refusal to suppress juvenile's confession notwithstanding arresting officer's failure to comply with parental notification provisions of FJDA, where circumstances surrounding the confession demonstrated voluntariness of juvenile's confession) *with United States v. Juvenile (RRA-A)*, 229 F.3d 737 (9th Cir. 2000) (ruling that juvenile's confession should be suppressed where arresting officer's failure to inform parents may have been a factor in confession, notwithstanding juvenile's request to arresting officers that her parents *not* be contacted and informed of the arrest).

Consider also the case of a juvenile in a foreign country who uses the Internet to damage a government computer or an e-commerce web server. Ordinarily, extradition of foreign nationals to the United States is governed by treaty. Some extradition treaties contain provisions that specifically permit the foreign sovereign to take account of the youth of the offender in deciding whether to extradite. *See, e.g.*, Convention on Extradition Between the United States and Sweden, 14 U.S.T. 1845; T.I.A.S. 5496 (as supplemented by Supplementary Convention on Extradition, T.I.A.S. 10812). Other treaties are silent on the issue of juveniles. How these situations will unfold in the future is unclear. Prosecutors who encounter situations involving network crimes by juveniles operating from abroad, should, in addition to consulting with Domestic

Security Section, consult with the Department's Office of International Affairs at (202) 514-0000.