It's Not Just Fun and "War Games" -- Juveniles and Computer Crime

Joseph V. DeMarco
Assistant United States Attorney
Southern District of New York
Computer and Telecommunications Coordinator

I. Introduction

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 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 PC'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's reply: *"Not if you are under eighteen."*

This article demonstrates why Broderick was wrong, for, while the movie may have seemed to be pure science fiction, the increased reliance on computers at all levels of society, coupled with the explosive growth in the use of personal computers and the Internet by teens, has made the scenario portrayed by the film seem to be not so fictional. Consider the following cases:

* A juvenile in Massachusetts pleads guilty to charges he disabled a key telephone company computer servicing the Worcester airport control tower, thereby disabling both the main radio transmitter, as well as a circuit which enabled aircraft on approach to send signals activating the runway lights.

* A 16-year-old from Florida pleads guilty and is sentenced to six months in a detention facility for intercepting electronic communications on military computer networks and for illegally obtaining information from a NASA computer network.

* A 16-year-old in Virginia pleads guilty to computer trespassing after hacking into a Massachusetts Internet service provider's (ISPs) computer system, causing $20,000 in damages.

* A 13-year-old California boy pleads guilty to making threats directed against a 13-year-old girl over the Internet. The boy had created a website which included a game featuring the girl's picture over a caption which read: "Hurry! Click on the trigger to kill her." The website included a petition calling for the girl's death.

See www.cybercrime.gov/juvenilepld.htm (Worcester airport); www.cybercrime.gov/comrade.htm (NASA case) Arthur L. Bowker, *Juveniles and Computers: Should We Be Concerned,* Federal Probation, December 1999, at 40 (Virginia and California cases).

This article seeks to explain: (1) why and how the rise of the computer culture and Internet generation presents opportunities for juveniles to commit crimes distinctly different from those traditionally committed by minors; (2) the statutory framework governing prosecution of computer delinquents in federal court; and (3) special considerations which pertain to the prosecution of computer crimes by juveniles. At a time when a *Newsweek* survey estimates that almost eighty percent of children regularly go online, the incidence of computer crime committed by juveniles will, increasingly, come to a prosecutor's attention.

II. Kids and Computer Crime

As has been documented in other articles in this publication, the rapid growth in the use of personal computers (PCs) and the advent of the Internet have made it possible for persons of all ages to commit serious crimes -- including extortion, computer hacking, and credit card fraud -- without ever leaving the comfort of home. In addition, difficulties in obtaining electronic evidence and tracing back to the electronic wrongdoer present unique challenges to law enforcement investigating computer crimes committed by persons of any age. In the context of juveniles who engage in criminally antisocial computer behavior, these problems take on special significance. This is true for several reasons.

First, the enormous computing power of today's PCs make it possible for minors to commit offenses which are disproportionately serious to their age. For example, while property offenses committed by minors in the "brick and mortar" world typically include shoplifting or other forms of simple theft, the advent of computer technology has made it possible for minors in the "point and click" world to engage in highly complex fraud schemes. "Typical" computer crimes committed by minors include trading stolen credit card numbers and amassing thousands of dollars worth of fraudulent purchases on those cards, or large-scale pirating of copyrighted computer software which is later sold or bartered to other minors in exchange for other pirated software. A Canadian juvenile has already been held responsible for launching a massive denial of service attack costing American companies millions of dollars. Likewise, there is, in principle, no reason why a juvenile could not release a computer virus, infecting tens of thousands of computers, or engage in large scale securities manipulation, causing six and seven-figure damages to investors. Indeed, given the technological sophistication of today's youth (evident to any parent who has relied on their fourteen year-old to set up the family computer), it is possible for a teenager to commit computer-related property offenses on a scale to which, prior to the 1980's, only seasoned veterans of the criminal justice system could aspire.

Second, the ability of a juvenile to portray himself or herself as an adult in the online world means that juveniles have access to fora in which to engage in criminal activity -- for example, auction Websites, financial services Websites, and chat rooms -- that in the physical world would quickly deny them any access at all. This access opens doors to criminality previously closed to minors. In a similar vein, kids who are too young to drive can use a PC connected to the Internet to access computers worldwide, adding to their ability to commit serious and far-reaching offenses and to confederate with other computer delinquents. Not only is it difficult for parents to deny their children access to computers -- necessary for much legitimate schoolwork -- even were parental control at home practicable, the ubiquitous (and often free) computer access provided by high schools, public libraries, and friends make "computer curfews" an oxymoron.

Third, juveniles appear to have an ethical "deficit" when it comes to computer crimes. In one study, 34 percent of university undergraduates admitted to illegally pirating copyrighted software, and 16 percent admitted to gaining illegal access to a computer system to browse or exchange information. *See* Bowker, *Juveniles and Computers*, at 41 (citing surveys). Moreover, a recent poll of 47,235 elementary and middle school students conducted by Scholastic, Inc. revealed that 48% of juveniles do not consider hacking to be a crime. This ethical deficit increases the likelihood that even "good kids" who are ordinarily unlikely to commit crimes such as robbery, burglary, or assault, may not be as disinclined to commit online crimes.

III. Prosecuting Juveniles in Federal Court

Against this backdrop, Federal prosecutors bringing computer delinquents to justice must master the provisions of the criminal code applicable to those actions. Specifically, they must understand the Juvenile Justice and Delinquency Prevention Act (the "Act"), codified at 18 U.S.C. §§ 5031 to 5042 of Title 18, which governs both the criminal prosecution or the delinquent adjudication of minors in federal court. While a complete analysis of the Act is beyond the scope of this article, certain of its provisions bear discussion, for proceedings against juveniles in federal court differs in significant respects from the prosecution of adults, and the prosecution of computer delinquents presents special considerations different from juveniles involved in other delinquencies. Specifically, as described below, the Act creates a unique procedure for delinquency proceedings against juveniles -- a process quasi-criminal and quasi-civil in nature, replete with its own procedural complexities and particular rules. In their totality, these

unique provisions seek to take account not only of the special protections provided to minors but also of the fact that even persons under 18 can commit "adult" crimes.

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 Act can be examined.

A. Who Is A Juvenile?

Under the Act, 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 do not apply at all. 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) (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) (absent improper delay by government, age at time of filing of formal charges determines whether the Act applies).

B. Does Federal Jurisdiction Exist?

As is true in the case of adults, not every criminal act 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 Act, there are three situations where federal delinquency jurisdiction over a juvenile exists. *First*, where the state court lacks jurisdiction, or refuses to assume jurisdiction. *See* 18 U.S.C. § 5032. *Second*, where the state does not have available programs and services adequate for the needs of juveniles. *See id. Third*, 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 there exists a sufficient federal interest to warrant exercise of federal jurisdiction. *See id.* These three jurisdictional bases are discussed below.

1. 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 computer delinquents. 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 a proceeding under its law against the minor. With regard to the former, although many states have enacted laws analogous to the general federal computer crime statute (18 U.S.C. § 1030), the electronic eavesdropping statute (18 U.S.C. § 2511), and the access device fraud statute (18 U.S.C. § 1029), to pick the most commonly prosecuted cybercrimes, some states do not have laws under which the crime in question can be prosecuted. In these cases, under the Act, the juvenile, nevertheless, can be held to account for his or her act of delinquency under federal law.

More commonly, however, a state will have a statute which does cover the cybercrime in question, *see, e.g.*, N.Y. Penal Law § 156.10 (computer trespass); *id.* § 156.27 (computer tampering in the first degree); *id.* § 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 and/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 cybercrime, 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 Act, however, does not appear to require that, in such cases, the government must certify that each and every state that could potentially have jurisdiction is unwilling to assume the jurisdiction at their disposal. The Act 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 supplied). 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, since federal criminal proceedings can often preclude state criminal proceedings under state double jeopardy principles, federal prosecutors faced with multi- state 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 provisions of the Act (discussed below) which deal with transfer of a juvenile to adult status.

2. The State Has No Programs or Inadequate Programs: This second basis for federal jurisdiction arises infrequently, as most states do have programs and facilities which provide for the adjudication, detention, and rehabilitation of minors. (Indeed, as of the writing of this article, there are no federal detention facilities specifically designed for juveniles. Juveniles who are the subject of federal delinquency proceedings are housed in contract facilities run by state, local, or private entities.) However, in the event that state officials were, for any reason, unable to address the needs of a juvenile, this exception would apply.

3. Enumerated Crimes and Crimes of Violence: Finally, the Act also sets forth certain federal crimes for which jurisdiction is deemed to exist, and where there is a substantial federal interest to warrant jurisdiction. The enumerated offenses are controlled substance offenses arising under 21 U.S.C. §§ 841, 952(a), 953, 955, 959, 960(b)(1), (2), (3), as well as firearms-related offenses arising under 18 U.S.C. §§ 922(x), 924(b), (g), or (h). While these offenses are typically inapplicable to cybercrime, the statute also permits jurisdiction in cases of "crimes of violence" which are punishable as felonies. *See* 18 U.S.C. § 5032. Although the Act itself does not define it, 18 U.S.C. § 16 defines crimes of violence as offenses that "ha[ve] as an element the use, attempted use, or threatened use of physical force against the person or property of another," or 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 commission of committing the offense." 18 U.S.C. § 16. In the context of cybercrime, the statutes which implicate this basis of jurisdiction include 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, *inter alia,* 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 warrants assumption of 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 it is not the victim, federal interests often exist, as cybercrime often involves conduct affecting critical infrastructures (*e.g.,* telecommunications systems); industries, or technologies significant to the nation's economy (*e.g.,* aerospace, computer software); or criminal groups operating in multiple states and/or foreign countries (*e.g.,* identity theft and stolen credit card rings). It is precisely in these important and often hard-to-enforce-locally situations that federal jurisdiction is peculiarly appropriate.

C. 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, ¶¶ 2-3. 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 Attorneys to sign the certification should be attached to the submission. (A copy of the delegation memorandum, dated July 20, 1995, can be obtained from the Terrorism and Violent Crime Section of the Department of Justice.)

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. And in that trial -- in which the government must prove that the juvenile has committed the act of delinquency beyond a reasonable doubt -- 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 their application is not inconsistent with any provision of the Act. *See* Fed. R. Crim. P. 54(b)(5); *see also* Wright, *Federal Practice and Procedure: Criminal 2d* § 873. The Federal Rules of Evidence likewise apply to the delinquency trial, *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 (3rd Cir. 1994) (collecting cases).

In addition, the Act affords juveniles special protections not ordinarily applicable to adult defendants. Most notably, the juvenile's identity is to be 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, whenever 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 they would have regular contact with adults. *See* 18 U.S.C. §§ 5035, 5038. Under the Act, a juvenile has a right to counsel at all critical stages of the proceeding, and the Act authorizes the appointment of counsel where the juvenile's parents or guardians cannot afford to retain counsel. *Id.*

D. Transfers From Juvenile Delinquency Proceedings 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 never be housed with adults, either pretrial or to serve a sentence. Most notably, 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, ¶ 4. In addition, the Act creates two forms of transfer which do not take into account the juvenile's wishes: 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 age fifteen or older at the time of the commission of the act of delinquency. *See* 18 U.S.C. § 5032, ¶ 4. As applied to the field of cyber- delinquency, it is available in

cases involving felony crimes of violence (*e.g.*, extortion, bomb threats). Under the Act, 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 juveniles behavioral problems. *See* 18 U.S.C. § 5032, ¶ 5. 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 cyber-delinquents come from middle- class, or even 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 under eighteen by only a few months and, as verge-of-adult wrongdoers, may well merit adult justice.

Mandatory transfer is more circumscribed than discretionary transfer, and is limited to certain enumerated offenses (*e.g.,* arson) which are not typically applicable in cyber-prosecutions, or to violent felonies directed against other persons. *See* 18 U.S.C. § 5032, ¶ 4. Here, however, transfer is further limited to offenses committed by juveniles age sixteen and older who also have a prior criminal conviction or juvenile adjudication for which they could be subject to mandatory or discretionary transfer. As a practical matter, therefore, in the area of cybercrime the majority of proceedings begun as juvenile proceedings will likely remain as such, and will not be transferred to adult prosecutions.

E. Sentencing And Detention

Under the Act, a court has several options in sentencing a juvenile adjudged to be delinquent. The court may suspend the finding(s) 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 they been an adult. *See* 18 U.S.C. § 5037(b). Accordingly, the Sentencing Guidelines, although not controlling, must be consulted. U.S.S.G. § 1B1.12; *see 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 they 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 they would be as an adult sentenced under the Guidelines. *See* 18 U.S.C. § 5037(b), (c).

IV. Special 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 United States Attorney's Manual provisions concerning delinquency proceedings, *see* USAM § 9-8.00, as well as the Terrorism and Violent Crime Section (TVCS), 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 ALR Fed. 481 (1997).

In addition to the novel nature of the proceedings themselves, however, 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 investigations of adults. Indeed, a seemingly routine post-arrest interview may raise issues of consent and voluntariness when the arrestee is a juvenile which are not present in the case of an adult arrestee. *Compare, e.g., 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 Act, where circumstances surrounding 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 parent's *not* be contacted and informed of the arrest).

Alternatively, consider the case of a juvenile in a foreign country who, via the Internet, does serious damage to a United States Government computer or to an e-commerce Webserver. Ordinarily, of course, extradition of foreign nationals to the United States is governed by treaty. Where they exist, treaties generally fall into two categories: "dual criminality" treaties, in which the signatories agree to extradite for offenses if the offenses are criminal in both nations, and "list" treaties, in which extradition is possible only for offenses enumerated in the treaty. Interestingly, however, some extradition treaties contain provisions which specifically permit the foreign sovereign to take account of the youth of the offender in deciding whether to extradite. *E.g.,* Convention on Extradition between the United States of America and Sweden, 14 UST 1845; TIAS 5496 (as supplemented by Supplementary Convention on Extradition, TIAS 10812). How these international juvenile delinquency situations will unfold in the future is unclear. What is clear is that as more and more of the planet becomes "wired," opportunities for cybercrime -- including cybercrime by juveniles -- will only increase. (Prosecutors who encounter situations involving juvenile's operating from abroad should, in addition to consulting with TVCS, consult with the Department's Office of International Affairs.)

V. Conclusion

Whether investigating a juvenile who commits a cybercrime involving computers maintained by a private party or computers maintained by segments of the strategic triad, a prosecutor considering bringing a juvenile to justice must not only master a new area of law, but also must be aware that traditional approaches to a case bear reevaluation in light of the unique aspects and special considerations presented by a juvenile who engages in acts of cyber- delinquency.

ABOUT THE AUTHOR

Joseph V. De Marco is an Assistant United States Attorney for the Southern District of New York, where he serves as Computer and Telecommunications Coordinator. Currently, he is on detail to the Department's Computer Crimes and Intellectual Property Section in Washington, D.C.