Juveniles and Computers: Should We Be Concerned?

By Arthur L. Bowker, M.A.
Computer Crime Information Coordinator, Northern District of Ohio

JUVENILE DELINQUENCY and its rehabilitation have been studied extensively over the years. Much of the interest in this topic has centered around the possible escalation of delinquent acts into adult criminal behavior and the impact of delinquent acts on society, particularly violent and drug offenses. Federal corrections have not been as focused on juvenile delinquency as in years past, due in large part to the small number of federal juvenile offenders. The advent of the computer delinquent* may change many of the concepts of juvenile offenses and rehabilitation, including the lack of federal interest. Consider for a moment the following comments of U.S. Attorney for the District of Massachusetts Donald Stern:

> Computer and telephone networks are at the heart of vital services provided by the government and private industry, and our critical infrastructure. They are not toys for the entertainment of teenagers. Hacking a computer or telephone network can create a tremendous risk to the public and we will prosecute juvenile hackers in appropriate cases, such as this one. (*Newsbytes News Network*, March 26, 1998)

In May of 1998, the first federal prosecution of a juvenile computer crime occurred in the District of Massachusetts. Subsequent federal prosecutions of computer delinquents occurred in the Southern District of New York, the Northern District of California, and the Northern District of Alabama. By the end of 1998, at least five juveniles had been federally prosecuted for offenses ranging from stealing passwords to hacking computers at the Pentagon and NASA, to accidentally shutting down an airport's runway lights and communications. Based upon 1995 figures, this represents 4 percent of all juveniles adjudicated federally and 19 percent of all delinquents federally adjudicated for property offenses (BJS, 1997).

But is this really the start of the federalization of the computer delinquent? Martha Stancelgen, Deputy Chief in the Computer Crime Section, U.S. Department of Justice, notes that federal prosecution of juveniles for computer offenses may be necessary. Specifically:

> I think for many federal prosecutors and investigators, pursuing cases that involve juveniles looks like not very serious work. It looks as if those cases don't merit the same sort of attention as offenses committed by adults. Well, we want our prosecutors and our agents to feel, to understand, that time invested in these cases is time very well spent, because juveniles have the skill and some of them will do a lot of damage.(Adams, Rajaun, and Wertheimer, 1999)

***Computer delinquency in this article refers to any delinquent act committed by a juvenile where a computer was the tool used in the offense, the target of a delinquent act, or contains evidence of a delinquent act.**

There are also signs that computer delinquents are having an impact on state juvenile justice systems. Consider the following cases:

- A 16-year-old in Chesterland County, Virginia pleaded guilty to computer trespassing for hacking into a Massachusetts Internet provider's system, causing $20,000 in damages (*Richmond Times-Dispatch*, June 25, 1999).
- Two youths, ages 14 and 17, pleaded guilty to charges that they scanned real money and printed counterfeit money in Bedford County, Virginia (*Roanoke Times & World News*, May 28, 1999).
- A 13-year-old boy from Pomona, California admitted to making threats against a 13-year-old girl with a computer. The boy had created a website which included a game featuring the girl's picture with the caption: "Hurry! Click on the trigger to kill her." The website also included a petition calling for her death (*San Diego Union Tribune*, May 9, 1999).
- A 14-year-old boy in Mount Prospect, Illinois pleaded guilty to possession of child pornography. The boy was downloading child pornographic images onto his computer (Gordon, 1999).

There are numerous factors that combine to make the computer delinquent a serious topic for corrections officials. Technologically, young people are more advanced than any previous generation. Specifically, advances such as the personal computer and the Internet have been today's reality for over 15 years—that's as far back as today's youth can remember. As a result, today's young people have a firm grasp of the potentials of these and other new technologies. In addition, an increasing number of juveniles have direct access to a computer and the Internet. According to Newsweek, 47 percent of the nation's teenagers were using computers to go online in 1999. Newsweek (1999) projects that by the year 2002 almost 80 percent of the nation's teens will be online. Unfortunately, the same article reports that many parents do not provide careful oversight of this computer use. Depending upon the age group, 9 to 38 percent of these youths have their parents sitting with them while they are online. Between 43 and 68 percent of parents of online children know which websites their children are visiting. In addition, between 54 and 75 percent of the parents permit online access whenever their children want.

Young people also seem to show an ethical deficit regarding the appropriate use of a computer. For instance, a recent study by Fream and Skinner (1997) of 581 undergraduate students found that 34 percent had pirated software in the previous year. Sixteen percent had gained illegal access to a computer system to either browse or exchange information. This study confirmed the extent of illegal computer use by college students that another study done five years earlier uncovered. Fream and Skinner's analysis revealed that parents and even teachers, by word and action, may be advocating the commission of certain computer crimes—most notably, software piracy—and this may increase the frequency of piracy and other computer crimes among the students. The study also noted:

> As with other types of deviance, one of the major predictors of computer crime is associating with friends who engage in the activity. Friends who are successful at certain activities or in scholastic areas are generally the ones whom other students seek out for help and advice. Also, friends are usually more willing to share such information or challenge others to beat them at their new games, programs or techniques. Thus, it comes as no surprise that learning computer crime is primarily peer driven. (Fream and Skinner, 1997, p. 503)

In years past the peer culture that most directly impacted youth was school and neighborhood friends. With the advent of the Internet, the peer culture does not have to be so close in proximity. There are numerous websites advocating such social plagues as pedophilia, drugs, and hate and racist groups. In addition, there are websites and chat rooms that are devoted to computer hacking and at least implicitly support the break-in of computer systems. McEwen (1991) notes with regard to hackers:

> …young hackers' beliefs about computers and information come from associations with other hackers, not family members and teachers. Few schools teach computer ethics, and parents of arrested hackers are usually unaware that their children have been illegally accessing computer systems.

Computers also provide delinquents with numerous opportunities that were unavailable in the past. Specifically, the use of the computer over the Internet can conceal age and provide a degree of anonymity that was previously impossible. It also opens up the range and scope for delinquent behavior. For instance, a youth who is not old enough to drive can use his or her computer to break into a computer several states away or even in another country. Young people can commit break-ins from their bedrooms, after curfew. Additionally, the power of the computer makes offenses that once required massive printers, such as counterfeiting or check fraud, now literally "child's play."

Because of our society's increasing dependence upon computers, the losses or damages that can be inflicted by a delinquent have dramatically changed. Losses, injuries, and/or deaths due to the acts of one delinquent have typically been quite low. In the past it was practically impossible for a juvenile delinquent to steal the amount of funds that a white-collar criminal, such as an embezzler, could purloin. However, a delinquent today can easily use a computer to facilitate a five-figure fraud or other high-tech crime (*Associated Press*, 1997). Even more horrific is the potential loss of life. For instance, a disturbed youth could use a computer to disrupt safety functions, such as traffic signals, air traffic control, or floodgates, making recent school massacres pale in comparison.

Indirect costs due to computer delinquency are also worth noting. Supposedly "innocent" juvenile exploration into computer systems can cause expensive systems to crash and inflict financial costs to bring the systems back. Because of the prevalence of computer intrusions, companies are required to take additional security measures, adding to the cost of goods and services. Computer delinquency also wastes investigative resources that could be better utilized. For instance, a computer attack against defense computers could be the work of a juvenile "exploring" or an adult terrorist bent on destroying systems or stealing technology. Only a costly investigation can tell. The expense and the "substantial federal interest" (see 18 U.S.C. §5032) make it more than likely that these young offenders will be prosecuted federally.

The jurisdictional concerns of technological crimes also make adjudicating computer delinquents even more complicated than the typical delinquency case. Normally, adjudicating a delinquent takes place at the local level. Juveniles usually lack the means to travel great distances to commit crimes unless they are engaged in stealing cars. A juvenile hacker can cross state boundaries and even international boundaries with ease. Who handles the case: the local authorities where the juvenile resides or the state or country of the target computer? Also, is there some federal interest in prosecuting the case? Is one of the correctional systems better equipped than others to deal with the supervision of this type of delinquent? Who decides which jurisdiction will prosecute the case and later supervise the delinquent after adjudication?

Finally, some computer delinquents are likely to become adult computer offenders. For instance, Kevin Mitnich, currently in federal custody for his second federal computer offense, started hacking at the age of 17 (Shimomura and Markoff, 1996). Another federal computer offender, Mark Abene of Masters of Deception infamy, also started computer offending at a young age (Quittner and Statalla, 1996). Robert J. Morris, the college student who released a "worm" that crashed approximately 6,000 computers on the Internet, began hacking into university computers as a juvenile (Hafner and Markoff, 1995). McEwen (1991) indicates:

> One conclusion from the studies is that persons involved in computer crimes acquire their interest and skills at an early age. They are introduced to computers in school, and their usual "career path" starts with illegally copying computer programs. Serious offenders then get into a progression of computer crimes including telecommunications fraud (making free long distance calls), unauthorized access to other computers (hacking for fun and profit), and credit card fraud (obtaining cash advances, purchasing equipment through computers). (p.9)

With these issues in mind, how does the typical probation officer, who may be barely computer literate, supervise a juvenile hacker, who can write his own software programs? One easy answer is to prohibit the delinquent's

access to a computer. But how does that impact the youth's education and development in a society that values computer proficiency? Is this a realistic condition for a delinquent with easy access to computers at home, schools, libraries, etc.? Will traditional efforts at rehabilitation work with computer delinquents? Are they different from the "traditional" juvenile offender, and if so how? Will the explosion of new technologies bring an increase in computer delinquency? These are questions that both federal and state corrections need to consider.

Obviously, the best solution is to prevent youth from gravitating into computer delinquency. Some efforts have been made to instill appropriate computer behavior in our youth. In 1990, the National Institute of Justice, with the cooperation of the U.S. Department of Education (DOE), invited concerned parties representing education, industry, law enforcement, and the government to a two-day meeting to address ethical issues surrounding technology. The group reached a consensus that ethics regarding the new technologies needed to be instilled in our youth. Specifically:

> With the rapid infusion of computers, software and related technologies into homes, schools and businesses, we initially focused our energies on learning about the technologies and how to use them. We now need to focus our attention on the ethical issues surrounding technology to insure that we and our children understand and practice values important to all of us—respect for others, their property, ownership, and the right to privacy. (Alden)

In response to this conference, the Computer Learning Foundation (CLF) (http://www.computerlearning.org), with DOE and the Department of Justice (DOJ), began emphasizing the need to teach responsible computer use to children. In 1991, the CLF began disseminating information to schools on methods for teaching children to be responsible computer users. In addition, the CLF developed the Code of Responsible Computing (Figure 1). Both the DOJ and the FBI's websites (http://www.usdoj.gov and http://www.fbi.gov) have pages for kids covering appropriate computer use. DOJ's website also has a lesson plan for elementary and middle school teachers to use when covering computer crime and ethics with their pupils.

As "agents of change" we need to be prepared at both the state and federal level when efforts at preventing computer delinquency have failed. Only additional study and focus on this new area of delinquency will arm us with the information and strategic thinking to cope with this new generation of delinquency.

FIGURE 1

CODE OF RESPONSIBLE COMPUTING

Respect for Privacy

I will respect others' right to privacy. I will only access, look in or use other individuals' organizations' or companies' information on computer or through telecommunications if I have the permission of the individual, organization or company who owns the information.

Respect for Property

I will respect others' property. I will only make changes to or delete computer programs, files or information that belong to others, if I have been given permission to do so by the person, organization or company who owns the program, file or information.

Respect for Ownership

I will respect others' rights to ownership and to earn a living for their work. I will only use computer software, files or information which I own or which I have been given permission to borrow. I will only use software programs which have been paid for or are in public domain. I will only make a backup copy of computer programs I have purchased or written and will only use it if my original program is damaged. I will only make copies of computer files and information that I own or have written. I will only sell computer programs which I have written or have been authorized to sell by the author. I will pay the developer or publisher for any shareware programs I decide to use.

Respect for Others and the Law

I will only use computers, software, and related technologies for purposes that are beneficial to others, that are not harmful (physically, financially, or otherwise) to others or others' property, and that are within the law.

References

Adams, Noah, Rajavan, Chitra, and Wertheimer, Linda, "Juvenile Cybercrime," *All Things Considered* (NPR), June 22, 1998.

Alden, Sally. Computer Learning Foundation Emphasizes Responsible Use of Technology http://wwwcomputerlearning.org/articles.

Bureau of Justice Statistics (BJS) (February 1997), *Juvenile Delinquents in the Federal Criminal Justice System*. Washington D.C.: U.S. Department of Justice.

"Chesterfield Youth Pleads Guilty to Hacking" (1999, June 25, 1999), *Richmond Times-Dispatch*.

Computer Learning Foundation (http://www.computerlearning.org/RespCode.html), Code of Responsible Computing.

Festa, Paul, "DOJ Charges Youth in Hack Attacks" (1998, March 18), *CNETNews.com*.

Fream, A.M and Skinner, W.F, "Social Learning Theory Analysis of Computer Crime Among College Students," *Journal of Research in Crime and Delinquency*, Volume 34, Issue 4, November 1997, pp. 495–518.

Gordon, Tony, "Mount Prospect Boy Pleads Guilty to Downloading Child Pornography" (1999, April 10), *Daily Herald*.

"Hacker Pleads Guilty to Stealing AOL Passwords" (1998, June 30), Bloomberg News/The Arlington News.

"Hackers Take Innocent Route Over ViRii Arrests" (1998, March 26), *Newsbytes News Network* (http://www.newsbytes.com).

Hafner, Katie and Markoff, John, *Cyberpunk:Outlaws and Hackers on the Computer Frontier*, Touchstone: New York, 1995, pp. 276–321.

"Judge Doesn't Convict Teen on Counterfeiting Charge, 2 Bedford County Students Charged for Fake Bills" (1999, May 28), *Roanoke Times & World News*.

McEwen, J. Thomas, "Computer Ethics," National Institute of Justice Reports, January/February 1991, pp. 8–10.

"NASA Nabs E-Mail Bomb Hacker" (1998, April 27), *Newsbytes News Network* (http://www.newsbytes.com).

"Online Threats Nets Probation" (1999, May 9), *San Diego Union Tribune*.

"Peril and Promise: Teens by the Numbers" (1999, May 10), pp. 38–39, *Newsweek* (www.newsweek.com).

Quittner, Joshua and Statalla, Michele, *Masters of Deception: The Gang that Ruled Cyberspace*, HarperCollins: New York, 1996.

Shimomura, Tsutomu and Markoff, *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw*, Hyperion: New York, 1996, pp. 370–372.

"Teen Hackers Forget to Cover Their Tracks" (1997, August 28), *Associated Press*.

"Teen Hackers 'Smash and Grab' $20,000 Worth of Equipment in Net Heists" (1997, November 10), *Nando.Net/Reuters*.

"ViRii Members Pled Guilty to Infiltrating Computers" (1998, July 30), *Newsbytes News Network* (http://www.newsbytes.com).

"Withdrawal Ordered for U.S. Pentagon Hackers" (1998, November 6), *Reuters*.